I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Beyond *WarGames*: How the Computer Fraud and Abuse Act Should be Interpreted in the Employment Context

MATTHEW KAPITANYAN[1]

Abstract: The nation's most important computer crime statute, the Computer Fraud and Abuse Act of 1986 ("CFAA"), has made its way into the employment relationship. This has generated a surge of academic alarm and more than a few confused courts. The legal quandary, however, comes down to a single word: "authorization." What does it mean to have it? When does an employee lose it? And why should it matter if she does? Behind the term of art rests two lines of interpretation. While some courts have interpreted "authorization" narrowly, by equating it with physical access, others have employed a broad interpretation, drawing the fault lines along the doctrines of contract and agency law. Commentators have constructed a number of arguments to support each interpretation, but most have urged the adoption of a narrow interpretation of authorization. This article argues that this narrow approach is imprudent and misguided and that a broad interpretation focusing upon the intent of an employee targets the greater threat and comports with policy and congressional intent. Such an approach should be adopted via statutory amendment.

[1] J.D. 2011, Columbia University School of Law; B.A. 2006, Lehigh University (International Relations & Journalism/Communications). I would like to thank the *I/S* staff for its insightful guidance in allowing this article to reach its full potential, and my family for their love, support, and encouragement.

I. INTRODUCTION

Although originally designed to protect against computer hackers, the Computer Fraud and Abuse Act of 1986 ("CFAA"),[2] the primary federal computer crime law, has found its way into the realm of employment law in the past decade as a means for employers to protect sensitive business resources from rogue employees.[3] Its applicability in this context, however, has generated scholarly debate and a circuit split.[4] The controversy is rooted in the statutory text: The CFAA prohibits what it deems unauthorized access to computers. The term "authorization," however, is undefined. In attempting to interpret it, courts have generally employed two distinct approaches. While some courts have defined "authorization" as a term of art rooted in agency or contract law, viewing unauthorized access as a question of the employee's intent,[5] others, in a recent trend, have utilized a narrower definition, examining whether the employer actually had granted the employee technical access to a resource by, for example, providing the employee with a username and password to access a particular database.[6]

[2] 18 U.S.C. § 1030 (2008).

[3] *See* Pac. Aerospace & Elecs. Inc. v. Taylor, 295 F. Supp. 2d 1188, 1196 (E.D. Wash. 2003) ("Employers . . . are increasingly taking advantage of the CFAA's civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system."); Orin Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN L. REV. 1561, 1583 (2010) ("In the last five years, cases applying the CFAA to allegedly disloyal employees have become by far the most common type of CFAA case."). Some have referred to the statute as "by far the most important and influential computer misuse statute in the United States, if not throughout the world." Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass and Privacy*, 62 BUS. LAW. 1395, 1402 (2007).

[4] *See* Nick Akerman, *Will SCOTUS Rule on the Computer Fraud and Abuse Act?*, Sept. 24, 2009, NAT'L L.J., *available at* http://www.law.com/jsp/cc PubArticleCC.jsp?id=1202434043364. Several courts of appeals have reached incompatible conclusions. A number of district courts have disagreed with the agency theory approach discussed *infra*. *See, e.g.*, Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322 (N.D. Ga. 2007).

[5] *See, e.g.*, Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006). In addition to the Seventh Circuit, the First Circuit, see EF Cultural Travel BV v. Explorica Inc., 274 F.3d 577 (1st Cir. 2007), and the Fifth Circuit, see United States v. John, 597 F.3d 263 (5th Cir. 2010), generally follow this interpretation of authority.

[6] *See, e.g.*, LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009).

This article examines the role and application of the CFAA in the employment context, specifically as used against rogue employees. Moreover, this article offers a resolution of a pressing legal question: In the context of a private cause of action against a rogue employee, how should courts determine when conduct is "authorized" pursuant to the CFAA? Part II presents an overview of why the issue deserves attention and prompt resolution. This overview includes an overview of the CFAA's original purpose, subsequent amendments, and current statutory structure. Part III examines the use of the CFAA in the employment context. Two diverging interpretations of "authorization" are presented. Part IV reviews pertinent scholarly commentary. Part V is a critical appraisal of the countervailing interpretations. An interpretation of authorization focusing on employees' intent is advocated as better serving the needs of the employment relationship. Part VI concludes by suggesting legislative action as the preferred means by which to resolve the debate.

II. OVERVIEW OF THE COMPUTER FRAUD AND ABUSE ACT OF 1986

A. THE PROBLEM IN 2011

The issue of what constitutes authorization warrants consideration and resolution because a lingering circuit split has left the law in this area unsettled in a number of jurisdictions. Compounding this concern is the increased prevalence of internal data theft. A February 2009 study by the Ponemon Institute, a privacy and management research firm, examined data loss risk during downsizing and found that 59% of employees who leave or are asked to leave steal company data.[7] Moreover, 79% of these employees said their former employer did not permit them to leave with company data.[8] Finally, 67% of these respondents said they used their former employer's confidential, sensitive, or proprietary information to leverage a new job.[9] A large-

[7] Data Loss Risks During Downsizing, Ponemon Institute, Feb. 23, 2009, *available at* http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/Data%20Loss%20 Risks%20During%20Downsizing%20FINAL%201.pdf. Kevin Rowney, founder of the Data Loss Prevention arm of security firm Symantec, the study's sponsor, further noted that there would be a "surging wave" of such insider theft. Maggie Shiels, Workers 'stealing company data,' BBC News, Feb. 23, 2009, *available at* http://news.bbc.co.uk/2/hi/technology/7902989.stm.

[8] Data Loss Risks During Downsizing, *supra* note 7.

[9] *Id.*

scale data breach investigations report conducted by Verizon Business also found that insider breaches accounted for 18% of attacks, with the remainder coming from outside the firm.[10] Though the insider breaches were fewer in number than those caused by external sources, when they did occur, they were much larger than those caused by outsiders.[11]

These figures raise additional concerns in light of the current factual context. According to the Bureau of Labor Statistics, in October 2003 55.5% of the total workforce—approximately 77 million persons—used a computer at work.[12] Moreover, the economic downturn, which began in 2008, has led to significant reductions in the national workforce across many industries.[13] The law regarding information theft and destruction by rogue employees is likely to be utilized in a new wave of potential claims, as insider breaches are on the rise and expected to increase.[14] The malicious insider is one of the

[10] 2008 Data Breach Investigations Report, Verizon Business RISK Team, *available at* http://www.verizonbusiness.com/resources/security/databreachreport.pdf.

[11] *Id.* A supplement to the report further noted "breaches involving insider abuse often occur after the employee is terminated or notified of termination. 2009 Data Breach Investigations Supplemental Report, Verizon Business RISK Team, *available at* http://www.verizonbusiness.com/resources/security/reports/rp_2009-data-breach-investigations-supplemental-report_en_xg.pdf. For an interesting account of how security and data protection are viewed as a strategic business priority for management, see Business Case for Date Protection: A Study of CEOs and Other C-Level Executives in the United Kingdom, Ponemon Institute, Mar. 2010, *available at* https://www14.software.ibm.com/iwm/web/cc/imc/rational/papers/Business_Case_for_Data_Protection_UK.pdf. (finding that C-level executives believe prudent data protection practices can support key organizational goals such as compliance, reputation management, and consumer trust).

[12] *See* U.S. Bureau of Labor Statistics, Computer and Internet Use at Work in 2003, at 1 (2005), *available at* http://www.bls.gov/news.release/ciuaw.nr0.htm. Presumably, this figure has increased in recent years.

[13] At the time of this writing, the unemployment rate has hovered between nine percent and ten percent. *See* Motoko Rich, *Adding Jobs, but Not Many, U.S. Economy Seems to Idle*, N.Y. TIMES, Oct. 7, 2011, *available at* http://www.nytimes.com/2011/10/08/business/economy/us-adds-103000-jobs-rate-steady-at-9-1.html?_r=1&scp=3&sq=unemployment%20rate&st=cse (noting that the economy is not growing fast enough to bring down the unemployment rate, "which held steady at 9.1 percent . . .").

[14] *See* Maggie Shiels, Malicious insider attacks to rise, BBC News, February 11, 2009, *available at* http://news.bbc.co.uk/2/hi/technology/7875904.stm (reporting that Microsoft, the world's largest software maker, has warned companies to expect an increase in insider security attacks by disgruntled, laid-off workers).

most significant threats companies face because the malicious insider has relatively easy access to a company's most valuable assets and know exactly where to find them.[15] In contrast, outsiders, such as hackers, must conduct a fishing expedition to accomplish the same thing. The available data seem to suggest that public and private actors have mistakenly devoted their attention to thwarting allegedly sophisticated and menacing outsiders, when the greater threat lurks within businesses themselves.[16]

B. THE PROBLEM IN 1984

Before 1984, there was no specific federal legislation in the area of computer crime.[17] Enforcement against computer-related crime was pursued under statutes designed to prosecute other offenses.[18] This changed in 1984 with the Counterfeit Access Device and Computer Fraud and Abuse Act ("CADCFAA"), a provision of the Comprehensive Crime Control Act intended to address the unauthorized access and

[15] *See id.* (quoting Doug Leland, a Microsoft Identity and Security Unit manager); *see also* First Annual Cost of Cybercrime Study: Benchmark Study of U.S. Companies, Ponemon Institute, July 2010, *available at* http://www.arcsight.com/library/download/ponemon-2010-cost-of-cyber-crime-study (finding that information theft constitutes the highest external cost of cybercrime, and that malicious insiders account for a substantial measure of cyber attacks). The Cybercrime study found that 62% of U.S. firms surveyed had experienced attacks relating to malicious insiders, and that such insiders constituted the second highest average annualized cybercrime cost weighted by the frequency of attack incidents (viruses and worms constituted the highest). *Id.* Finally of note, attacks by malicious insiders took, on average across the firms surveyed, 30.4 days to resolve. Only malicious code attacks took longer to resolve (39.3 days). *Id.*

[16] *See* Shiels, *supra* note 14 (quoting Kevin Rowney of Semantec: "The outstanding, unsolved, unaddressed risk management problem that has existed for years is that everyone is focusing on the hacker[.] It feels more sexy and interesting to fend against the assailant from the outside rather than face the possibility that the guy in the next cubicle is ripping off corporate data.").

[17] H.R. REP. NO. 98-894 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3691-92. Note, however, that all 50 states have some sort of computer crime legislation. Some state legislatures enacted these statutes before the federal computer crime law. Florida passed the first. Vermont passed the last. *See* Orin Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1616 (2003).

[18] *See id.* (noting the use of the mail fraud (18 U.S.C. 1341) and wire fraud (18 U.S.C. 1343) statutes).

use of computers and computer networks.[19] Citing the technological transformation over the past 25 years and the integration of the computer into everyday lives, and as a critical component of national defense, financial transactions, and information transmission, the 1984 House Report supporting passage of the CADCFAA noted that "traditional theft/larceny statutes are not the proper vehicle to control the spate of computer abuse and computer assisted crimes."[20] Furthermore, the report found that the proliferation of computer networking since the 1970s had permitted hackers to access both private and public computer systems, with potentially serious results.[21] The report referenced the 1983 film, *WarGames*, in which Matthew Broderick played a computer hacker who infiltrates a confidential government system, gains complete control over the U.S. nuclear arsenal, and nearly causes a large-scale nuclear war.[22] The CADCFAA was introduced on the floor of Congress only months after the film's release.[23] Thus, it seems clear that hacking, and related computer misuse, served as a key impetus for the first federal computer crime statute.[24]

The legislative history supports the conclusion that Congress mostly saw the 1984 Act as doing for computers what trespass and burglary laws did for real property.[25] The statute essentially functions

[19] *See* Prosecuting Computer Crimes Manual, United States Department of Justice, February 2007, *available at* http://www.justice.gov/criminal/cybercrime/ccmanual/ccmanual.pdf.

[20] H.R. REP. NO. 98-894 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3694-95.

[21] *Id.*

[22] WarGames (MGM/UA Studios 1983).

[23] *See* Joseph M. Olivenbaum, *CTRL-ALT-DELETE: Rethinking Federal Computer Crime Legislation*, 27 SETON HALL L. REV. 574, 596 (1997) (noting that the House Report "specifically referred to testimony describing War Games as a 'realistic representation of the automatic dialing and access capabilities of the personal computer,' and thus, apparently, of the threat to computer security presented by those capabilities").

[24] Professor Kerr provides a useful dichotomy. The umbrella of computer crime can be divided into two types of substantive offenses: traditional crimes using computers, such as an online death threat, and crimes of computer misuse, such as hacking. Kerr, *supra* note 17, at 1602-05.

[25] *See id.* at 1617. The concept of trespass in cyberspace invokes a preliminary inquiry of whether a website or server should be deemed property. This is a contested theoretical issue that is beyond the scope of this article. For the purposes of this article, it may be assumed that Congress considered the activities of computer hackers to be akin to trespass,

like a federal claim for trespass[26] by prohibiting certain conduct involving unauthorized access to a computer system. The 1984 Act performed this function by prohibiting unauthorized access in three narrow areas.[27] Subsection 1030(a)(1) made it a felony to knowingly access a computer without authorization, or in excess of authorization, in order to obtain classified United States defense or foreign relations information.[28] Subsection 1030(a)(2) made it a misdemeanor to knowingly access a computer without authorization, or in excess of authorization, in order to obtain information contained in a financial record of a financial institution or in a consumer file of a consumer-reporting agency.[29] Finally, subsection 1030(a)(3) made it a misdemeanor to knowingly access a computer without authorization, or in excess of authorization, in order to compromise or affect the government's use of the computer.[30] These narrow proscriptions only protected certain types of computer systems and select types of information on those systems.[31] Congress believed that such computer

see H.R. REP. NO. 98-894 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3695 ("... so-called 'hackers' who have been able to access (trespass into) both private and public computer system. . ."), and the relevant digital information to be considered property, *see* S. REP. NO. 99-432, at 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2491 (recognizing the "necessity that computerized information be considered 'property' for purposes of Federal criminal law"). For commentary challenging the metaphor of the Internet as a "place" and thus warranting property-based rules, see, e.g., Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439 (2003); Mark A. Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521 (2003).

[26] *See* Maureen A. O'Rourke, Common Law and Statutory Restrictions on Access: Contract, Trespass, and the Computer Fraud and Abuse Act, 2002 U. ILL. J.L. TECH. & POL'Y 295, 308 (2002).

[27] *See* Dodd S. Griffith, Note, The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem, 43 VAND. L. REV. 453, 460 (1990).

[28] *See id.* at 461-62 (citing Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, ch. 21, 98 Stat. 2190 (1984) (codified as amended at 18 U.S.C. § 1030 (2008)).

[29] *See id.*

[30] *See id.*

[31] The 1984 Act applied to "federal interest computers." This term was defined as a computer exclusively for the use of a financial institution or the United States Government, or in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government. *See* Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control*

systems needed special protection because they contained the most sensitive types of information, particularly classified information, financial records, and credit histories.[32]

C. SUBSEQUENT EXPANSION OF THE ACT

Despite a fairly broad focus (i.e., computer crime), the 1984 Act was narrow in scope.[33] Instead of amending every statute affected by advances in computer technology, Congress chose to address the subject in a single statute but was reluctant to preempt or interfere with local and state computer crime authorities.[34] In addition to this deficiency, the statute was also criticized as being overly vague, incomplete, structurally flawed, and difficult to use.[35] In light of these shortcomings, Congress continued to investigate the problems associated with computer crime to determine if further revision was necessary.[36] Throughout 1985, congressional hearings were held focusing on the appropriate scope of federal jurisdiction in the area of computer crime. Although it was proposed, Congress declined to enact "as sweeping a federal statute as possible so that no computer crime is potentially uncovered."[37] The preferred approach, rather, was to limit federal jurisdiction over computer crime to cases presenting a compelling federal interest—where computers of the Federal

Information on Publicly Accessible Internet Websites, 63 MD. L. REV. 320, 327-28 (2004) (citing S. REP. NO. 104-357, at 4 (1996)).

[32] *See id.*

[33] *See id.*

[34] *See id.*

[35] *See* Reid Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 BERKELEY TECH. L.J. 909, 912 (2003); Griffith, *supra* note 27, at 466-74 (noting grievances and recommendations to the Act from multiple parties, including legislators, analysts, and state and federal law enforcement officials); *see also* Charlotte Decker, *Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime*, 81 S. CAL. L. REV. 959, 978 (2008) (noting that the lack of clarity in defining key terms, inability to react to changing technology, and failure to combat non-interstate computer crime doomed the success of the 1984 Act).

[36] *See* S. REP. NO. 99-432, at 1-2 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2479; Prosecuting Computer Crimes Manual, *supra* note 19 (tracing the 1984 Act's legislative evolution).

[37] S. REP. NO. 99-432, at 4.

Government or certain financial institutions were involved, or where the crime itself was interstate in nature.[38] Instead of incremental changes, however, the hearings culminated in a complete revision of the Act in 1986.[39] The CFAA was enacted to amend 18 U.S.C. § 1030.

The 1986 Act expanded the scope of the 1984 Act by adding three new felony offenses. Subsection 1030(a)(4) prohibits federal computer fraud.[40] Subsection 1030(a)(5) penalizes those who damage, alter, or destroy another's data.[41] Finally, subsection 1030(a)(6) criminalizes trafficking in computer passwords, among other things.[42] The new offenses required a heightened mens rea of "intentionally," as compared with "knowingly," the standard in the 1984 Act.[43]

The 1986 amendments also altered a number of provisions in the 1984 Act. Several are particularly noteworthy. Subsection 1030(a)(3) was modified to make unauthorized access alone a criminal offense.[44] The amendments also removed the use exemption that limited the application of subsections 1030(a)(2) and 1030(a)(3), and changed the mens rea requirements for those subsections from "knowingly" to "intentionally." In line with the heightened scienter requirement, the Senate Report noted that the 1986 amendments would:

[38] *Id.* Congress was satisfied that this approach struck "the appropriate balance between the Federal Government's interest in computer crime and the interests and abilities of the States to proscribe and punish such offenses." *Id.*

[39] *See* Skibell, *supra* note 35, at 912.

[40] *See id.* at 913 (citing S. REP. NO. 99-432, at 9). Though patterned after the mail and wire fraud statutes, this subsection was distinguished from those statutes by requiring the use of a computer for criminal liability to attach.

[41] *See id.* (citing S. REP. NO. 99-432, at 13, and noting that this was the most important addition provided by the 1986 amendments). This essentially made computer hacking a federal offense, and was designed to prohibit such activities as the distribution of malicious code and denial of service attacks. *See* Prosecuting Computer Crimes Manual, *supra* note 19. A denial of service attack is a hacking activity, which floods a victim computer with useless information and prevents legitimate users from accessing it. *Id.*

[42] *See* Skibell, *supra* note 35, at 913 (citing S. REP. NO. 99-432, at 13).

[43] *See id.* at 913-14 (citing S. REP. NO. 99-432, at 10). This was done to exempt those who might mistakenly access a protected computer or stumble upon another's data protection. *See id.* at 914 (citing S. REP. NO. 99-432, at 5-6).

[44] S. REP. NO. 99-432, at 6. This alleviated concerns as to whether simple trespass alone was a punishable offense, or if a further showing that the information accessed was used, modified, destroyed, or disclosed was necessary.

> eliminate coverage for authorized access that aims at 'purposes to which such authorization does not extend.' This [would] remove[] from the sweep of the statute one of the murkier grounds of liability, under which a Federal employee's access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization.[45]

Finally, the amendments established definitions for a number of key terms, including "exceeds authorized access," which was defined as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[46] The term "without authorization" has never been defined. However, the Senate Report supporting passage of the 1996 amendments to the CFAA suggests that persons who exceed authorized access are likely to be insiders, while persons who act without authorization are likely to be outsiders.[47]

Since 1986, the CFAA has been amended eight more times. Only one of these amendments, the 1994 revision, is pertinent for the purposes of this article.[48] The renewed concern underlying this revision once again was computer hackers, as Congress feared that loopholes in the statute permitted some hackers to avoid punishment.[49] Congress sought to expand the CFAA to give the

[45] S. REP. NO. 99-432, at 21. The Senate Report noted that administrative sanctions should be adequate to deal with real abuses of authorized access to Federal computers, and that this change minimizes the likelihood that a Federal employee, uncertain of his authority, would face a choice between disclosure mandates and criminal sanctions. *Id.*

[46] 18 U.S.C. 1030(e)(6). The Senate Report found these definitions "self-explanatory." S. REP. NO. 99-432, at 12.

[47] *See* Prosecuting Computer Crimes Manual, *supra* note 19. The report further notes: "[I]nsiders, who are authorized to access a computer, face criminal liability only if they intend to cause damage to the computer, not for recklessly or negligently causing damage. By contrast, outside hackers who break into a computer could be punished for any intentional, reckless, or other damage they cause by their trespass." S. REP. NO. 104-357, at 11 (1996).

[48] The CFAA was subsequently amended in 1988, 1989, 1990, 1994, 1996, 2001, 2002, and 2008. In 1994, Congress amended the CFAA as part of the Violent Crime Control and Law Enforcement Act of 1994. Computer Abuse Amendments Act of 1994, Pub. L. No. 103-322, § 290001, 108 Stat. 2097, (1994).

[49] *See* Galbraith, *supra* note 31, at 329.

government more power to thwart their efforts, and did three things of note.[50] First, a private right of action was added in subsection 1030(g).[51] Second, the statute's scope was expanded from "federal interest computers" to all "protected computers."[52] A "protected computer" was defined to include the previous definition of a "federal interest computer," as well as "a computer which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."[53] (Since the advent of the internet, however, almost all computer use has become interstate in nature.[54]) Finally, subsection 1030(a)(5) was amended to create two new substantive offenses—one for intentional acts, and the other for reckless acts.[55]

The legislative history reveals that Congress has deliberately broadened the CFAA several times since its inception only twenty-six years ago. Each revision since 1986 has widened the depth and breadth of the statute by adding substantive offenses, lowering levels of scienter, or increasing penalties.[56] Furthermore, Congress has instructed that future revisions keep pace with technological

[50] *See id.*

[51] Although a significant means of expansion, the civil remedy seems to have received little discussion in the Senate Report supporting passage of the 1994 amendment. *See* Kyle W. Brenton, *Trade Secret Law and the Computer Fraud and Abuse Act: Two Problems and Two Solutions*, 2009 U. ILL J.L. TECH. & POL'Y 429, 453 (2009).

[52] *See id.*

[53] 18 U.S.C. § 1030(e)(2)(B). Note that this was further amended in 2001 to include computers outside of the United States so long as they affect "interstate or foreign commerce or communication of the United States." *See* Prosecuting Computer Crimes Manual, *supra* note 19.

[54] *See* Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1127 (W.D. Wash. 2000); *see also* Kerr, *supra* note 3, at 1568 ("[I]t seems that every computer connected to the Internet is a "protected computer" covered by 18 U.S.C. § 1030.").

[55] *See* Skibell, *supra* note 35, at 914. Prior to this time, the CFAA did not punish unintentional damage caused while accessing a system. *Id.*

[56] *See id.* at 911 (citing U.S. v. Middleton, 231 F.3d 1207, 1212 (9th Cir. 2002), and noting that the consistent expansion of the statute has led at least one court to conclude that where there is ambiguity in the statute, Congressional intent should be presumed to support an expansive scope).

development, and new forms of computer misuse, through a malleable legal framework.[57]

D. STATUTORY STRUCTURE

The statute in its present form incorporates many of the revisions discussed above, as well as prior and subsequent amendments to the CFAA not explicitly mentioned. A review of the current statutory structure provides insight into which interpretation of authorization more naturally comports with textual considerations.

The CFAA establishes seven substantive offenses involving unauthorized access to computers[58] and, while the CFAA is a criminal statute, it provides a private cause of action.[59]

Authorization is an element in most of the substantive provisions. For instance, subsection 1030(a)(2) prohibits intentionally accessing a computer without, or in excess of, authorization and obtaining information from the financial records of a financial institution, the United States government, or a protected (e.g., private) computer used in interstate commerce.[60]

Subsection 1030(a)(4) is another subsection that is commonly evoked against rogue employees. This subsection prohibits knowingly accessing a protected computer without, or in excess of, authorization, with intent to defraud where such access furthers the intended fraud and the violator obtains anything of value, including use of the

[57] S. REP. NO. 104-357, at 5 ("As computers continue to proliferate in businesses and homes, and new forms of computer crimes emerge, Congress must remain vigilant to ensure that the Computer Fraud and Abuse statute is up-to-date and provides law enforcement with the necessary legal framework to fight computer crime. The [1996 amendments] will likely not represent the last amendment to this statute, but is necessary and constructive legislation to deal with the current increase in computer crime.").

[58] *See* 18 U.S.C. § 1030(a)(1)-(a)(7).

[59] 18 U.S.C. § 1030(g). The right of action contains a two-element injury prerequisite. First, a plaintiff must show she suffered damage or loss (as defined within the Act) as a result of a violation of the Act. *Id.* Second, the conduct alleged must involve one of the following: (1) loss to one or more persons during any one-year period aggregating at least $5,000; (2) modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more persons; (3) physical injury to any person; (4) a threat to public health or safety; (5) damage affecting a computer used by or for an entity of the U.S. Government in furtherance of the administration of justice, national defense, or national security. 18 U.S.C. § 1030(c)(4)(A)(i)(I)-(V).

[60] 18 U.S.C. § 1030(a)(2). Note also that "obtaining" information carries an expansive meaning, which includes the mere observation of data. *See* S. REP. NO. 99-432, at 6.

computer if the value of such use exceeds $5,000 in a one-year period.[61]

Subsection 1030(a)(5) addresses computer hacking and contains two categories of offenses which differ based on their respective mens rea requirements. Subsection 1030(a)(5)(A) prohibits *knowingly* causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causing damage, without authorization, to a protected computer.[62] This subsection applies regardless of whether the user had authorization to access the computer. Subsection 1030(a)(5)(B) prohibits *intentionally* accessing a protected computer without authorization, and as a result of such conduct recklessly causing damage. Subsection 1030(a)(5)(C) is nearly identical. However, it substitutes recklessness for the mens rea and requires that the violator cause damage and loss (loss is an added element).[63]

Subsections 1030(a)(1), 1030(a)(3), 1030(a)(6), and 1030(a)(7) are not frequently used against rogue employees. Additionally, the latter two subsections do not prohibit unauthorized access on its face and thus do not require it as a condition precedent for liability.

Section III proceeds to examine and appraise the alternative interpretations of authorization after reviewing the use of the CFAA in the employment relationship.

III. THE CFAA AND EMPLOYMENT

A. THE CFAA IN THE EMPLOYMENT RELATIONSHIP

Considering the extent to which the workplace has become digitalized, it is unsurprising that computer misuse by employees has emerged as a serious concern. Though employers may resort to state common law claims for relief (such as tortious interference with

[61] 18 U.S.C. § 1030(a)(4). Courts have interpreted fraud within the meaning of this statute broadly. *See* Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1126 (W.D. Wash. 2000). This interpretation, however, serves to balance a tight nexus implicit in this statute as compared to the sister mail and wire fraud statutes. Computer use that is extraneous to an intended fraud is not covered by subsection 1030(a)(4). It would be if this subsection was patterned directly after the mail and wire fraud statutes. *See* S. REP. NO. 99-432, at 9 ("To be prosecuted under this subsection, the use of the computer must be more directly linked to the intended fraud.").

[62] 18 U.S.C. § 1030(a)(5)(A).

[63] 18 U.S.C. § 1030(a)(5)(C).

business relations, theft of trade secrets, breach of employment contract, or breach of fiduciary duty), the CFAA provides an attractive alternative because it allows plaintiffs to bring claims against the former employee *and* her new employer, provides a basis for federal jurisdiction, and allows for injunctive relief. Moreover, the CFAA provides a remedy without requiring the employer to prove the breach of an employment agreement or that the data taken is secret or confidential.[64] Employers need only show unauthorized access to a protected computer and the requisite damages.

Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.[65] was the first case to apply the CFAA to the exploits of a rogue employee. After Congress established a private cause of action under the CFAA, and prior to *Shurgard*, most CFAA litigation focused upon unsolicited (and unauthorized) bulk email and closely related commercial disputes.[66] Until this time, employers had not turned to the CFAA for relief from harm caused by rogue employees.

The facts of *Shurgard* present the quintessential rogue employee fact pattern. Shurgard Storage Centers, Inc. was an industry leader in the full and self-service storage business, a high barrier to entry market.[67] Safeguard Self-Storage was its direct competitor.[68] Pursuant to its business strategy, Shurgard had developed a sophisticated system of indentifying target sites and assessing their economic value

[64] *See* Posting of Robert Milligan and Carolyn Sieve of Seyfarth Shaw to TradingSecretslaw.com, Oct. 28, 2009, *available at* http://www.tradesecretslaw.com/uploads/file/Establishing%20CFAA%20Violations%20-%20Law%20360.pdf; Peter J. Pizzi, *Disloyal Employees: Computer Abuse Law Turns on Meaning of 'Without Authorization,'* N.Y. L.J., Sept. 5, 2006, at 5 (noting the CFAA can provide a remedy against a former employee unavailable under state law in jurisdictions that refrain from enforcing non-compete agreements, such as California).

[65]*Shurgard*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000). Note that this case has been overruled to some extent by LVRC Holdings LLC v. Brekka, 581 F. 3d 1127 (9th Cir. 2009).

[66] *See, e.g.*, Cyber Promotions, Inc. v. Am. Online, Inc., 948 F. Supp. 436 (E.D. Pa. 1996) (e-mail bombing of competitor's internet service provider); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444 (E.D. Va. 1998) (unsolicited bulk e-mail); eBay, Inc. v. Bidder's Edge, Inc., 100 F.Supp.2d 1058, 1060 (N.D. Cal. 2000) (unauthorized use of automated querying program on plaintiff's website); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000) (unauthorized use of "search robots" to extract names of registrants from website).

[67] *Shurgard*, 119 F. Supp. 2d at 1122.

[68] *Id.* at 1122-23.

to its business model.[69] To this end, Shurgard invested significant resources in creating a marketing team to become familiar with potential target markets, identify potential sites, and develop key relationships with brokers and sellers in those markets.[70] This business strategy had allowed Shurgard to sustain its growth and development for twenty-five years.[71] Safeguard entered the market in 1997, three years before the disposition of the case, and two years before the events that precipitated the dispute.[72]

Eric Leland was a regional development manager for Shurgard.[73] On account of his position at Shurgard, he was entrusted with full access to the company's confidential business plans, expansion plans, and other trade secrets.[74] In 1999, Leland was approached by Safeguard and offered a position.[75] Shortly thereafter, while still employed by Shurgard, Leland sent e-mails containing Shurgard's trade secrets and proprietary information to Safeguard representatives without Shurgard's approval or knowledge.[76] Leland continued to supply Safeguard with this type of information after leaving Shurgard.[77] Shurgard sued Safeguard under subsections 1030(a)(2)(C), 1030(a)(4), and 1030(a)(5)(C), seeking damages and injunctive relief.[78] Shurgard argued that Leland's authorization ended when he began acting as an agent for Safeguard, making him unauthorized to access the information in question.[79] Safeguard contended in its defense that Leland had been given full access to the information in question and, thus, was not without, or in excess of,

[69] *Id.* at 1123.

[70] *Id.*

[71] *Id.* at 1122.

[72] *Shurgard,* 119 F. Supp. 2d at 1123.

[73] *Id.*

[74] *Id.*

[75] *Id.*

[76] *Id.*

[77] *Shurgard,* 119 F. Supp. 2d at 1123.

[78] *Id.*

[79] *Id.* at 1124.

authorization.[80] The litigants' positions depended upon different definitions of "authorization." While Shurgard employed a legalistic interpretation, relying upon agency law to define authorization,[81] Safeguard relied upon a narrow technological interpretation, which instead dictated that whoever is granted access as a preliminary matter is absolutely authorized to use that access, regardless of their purpose in doing so.[82]

The court looked first to the language of CFAA, noting that its unambiguous meaning should be the first and final inquiry unless it would lead to an absurd result.[83] Although it found the agency-based interpretation of authority to pass muster under this standard, and accepted it, the court examined the legislative history of the CFAA to determine whether it was appropriate to apply the statute to employees (i.e., insiders), in addition to outsiders (e.g., hackers).[84] The court noted that while the original scope of the statute was limited to outsiders, "its subsequent amendments have broadened the scope significantly to cover [rogue employees]."[85] The court found support for this interpretation of the legislative history in congressional reports demonstrating the broad meaning and intended scope of the terms "protected computer" and "without authorization," congressional intent to permit a CFAA claim to rest alongside a copyright claim, and intent to punish those who illegally use computers for commercial advantage.[86]

In reaching its conclusion to apply an agency-based interpretation of authorization, the court relied upon *United States v. Morris*.[87] In *Morris*, a computer user who was authorized to access a computer and its programs via an account with his university lost authorization

[80] *Id.*

[81] *Shurgard* cited to the RESTATEMENT (SECOND) OF AGENCY § 112 (1958) for this proposition.

[82] This has been referred to as a code-based interpretation of authorization. *See* Kerr, *supra* note 17.

[83] *Shurgard*, 119 F. Supp. 2d at 1124.

[84] *Id.* at 1127-29.

[85] *Id.* at 1127.

[86] *Id.* at 1127-29.

[87] United States v. Morris, 928 F.2d 504 (2d Cir. 1991).

when he used the programs in an unauthorized way.[88] The court reached this conclusion despite the fact that Morris had been working on a computer virus (a "worm") in order to demonstrate the inadequacies of current network security measures.[89] Morris took measures to minimize the worm's interference with the network it infiltrated, but the worm ended up causing havoc in many of the computers it infected.[90] In finding criminal liability under subsection 1030(a)(5)(A), the court reasoned that Morris's conduct fell well within the area of unauthorized access because while he was technically authorized to use the networks in question, he "did not use [the network features] in any way related to their intended function."[91]

[88] *Id.* at 505.

[89] *Id.*

[90] *Id.* at 506.

[91] *Id.* at 510. Furthermore, *Morris* presents a useful vantage point into the debate that will be explored in Part V *infra*. While the court acknowledged that Morris was explicitly authorized to use the computers in question, *id.* at 505, 509-10, it framed the question as whether his transmission of the worm constituted an act for which he was not authorized (or which exceeded his authorization). *Id.* at 510. In this endeavor, the court threaded a thin line. Although it rhetorically erected the framework of the narrow, code-based (or technological) definition of authority, the court relied upon a non-code-based system of social norms—what society considers an appropriate or inappropriate use of a computer—to reach its result. This seems to be the focus of the court's "intended function" test. *Id.* Commentators have thoughtfully expounded the ideological mechanism inherent in this test. *See* Winn, *supra* note 3, at 1408 ("What *Morris* . . .establish[es], then, is not so much a point of law, but a point of logic. Machines can authorize nothing. The idea of authorization necessarily requires reference to human beings—in particular, reference to a system of established rights and duties in a community[.] [M]achines alone cannot supply the law with a system of norms."); Kerr, *supra* note 17, at 1632 (noting that the intended function test "appears to derive largely from a sense of social norms in the community of computer users"). While it may be argued that "intended function" refers to the nature of Morris's access, and thus comports with a code-based understanding of authorization, under a code-based test such an inquiry is superfluous, as the court had already noted that Morris himself was authorized to use the computer. Therefore, the intended function analysis evaluated not Morris's access per se, but rather what he did with that access. Thus, it seems as though "intended function" served as a legal proxy used to assess the manner in which an actor utilizes the access he is granted, distancing the test from a pure code-based interpretation of authorization. Alternative understandings of the *Morris* approach, which seek to further unite its reasoning and outcome under the code-based umbrella, have also been suggested. *See* Katherine Mesenbring Field, Note, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 825 (2009) (finding *Morris's* intended function test to be similar to a code-based interpretation because violation of the intended function is often done through technical means, such as finding holes in programs, or bypassing passwords or other protection systems); United States v. Aleynikov, No. 10 Cr. 96(DLC), 2010 WL 3489383, at

The preliminary question of whether the CFAA can be applied in the employment context should be answered in the affirmative. The original House report supporting passage of the 1984 Act cited two cases to illustrate the necessity of a computer crime statute analogous to the mail and wire fraud statutes.[92] In the first case, a former employee used an active employee's username and password to tap into his former employer's computer system via remote terminal, and accessed confidential software.[93] In the second case, a former employee who was given daily access to the Federal Reserve Board's computer by telephone was apprehended and convicted when he continued to access the system using the access code of an unwitting colleague.[94] The fact that both of these cases involved access by employees, albeit former employees, indicates that Congress was not solely concerned with deterring hackers when it passed the original statute.[95] Even courts rejecting the *Shurgard* approach have noted that the employment relationship is an appropriate context for the statute's application. Both the *Black & Decker* and *US Bioservices* courts agreed with the *Shurgard* court that the CFAA's legislative history supports the proposition that the statute applies not only to "outsiders," but also to "insiders" such as present and former

*16 n. 24 (S.D.N.Y. Sept. 3, 2010) (noting that while Morris had authorization to access the university computer system, he acted without authorization when he exploited a special and unauthorized access route into other computers for which he had no authority). Indeed, the state of the law on this issue in the Second Circuit is somewhat in flux. *Compare Aleynikov*, 2010 WL 3489383, at *17 (authority not lost when employee misappropriated employer's information) *with* Mktg. Tech. Solutions, Inc. v. Medizine LLC, No. 09 Civ. 8122(LMM), 2010 WL 2034404, at *7 (S.D.N.Y. May 18, 2010) (employee's actions in contravention of employment agreement were in excess of authorization). As the *Aleynikov* decision highlights, it is also noteworthy that, as an alternative basis for its holding, the *Morris* court cited the lower court's finding that "the evidence also demonstrated that the worm was designed to spread to other computers at which [Morris] had no account and no authority, express or implied, to unleash the worm program." *Morris*, 928 F.2d at 510. Thus, in contrast to the primary basis for its holding, the court's alternative basis comports with a pure code-based interpretation of authorization.

[92] H.R. REP. NO. 98-894, at 6 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3691-92.

[93] United States v. Seidlitz, 589 F.2d 152, 153-55 (4th Cir. 1978).

[94] A summary of the relevant facts can be found at *Filching Figures*, TIME, Jan. 17, 1983, *available at* http://www.time.com/time/magazine/article/0,9171,951875,00.html.

[95] The 1996 Senate report shows similar intent to include employees within the CFAA's ambit. *See supra* note 47 and accompanying text.

employees.[96] The *Black & Decker* court further noted that the statutory structure provides additional support, as the statute "criminaliz[es] certain conduct committed by "whoever," [without] providing any affirmative defenses relating to "insider" status."[97]

Since 2000, courts have struggled with delineating a proper conception of authority within the meaning of the CFAA. Although *Shurgard* was the first case of its kind, it certainly has not been the only attempt to offer a viable interpretation of the elusive concept. The following subsection further explores the diverging paths in the interpretation of authority.

B. DIVERGING INTERPRETATIONS OF AUTHORIZATION

There is a split in legal authority as to whether an employee acts without authorization when he obtains data that he is entitled to access, but uses that data in a manner that is inconsistent with a contractual obligation (e.g., as set out in an employment agreement or employee handbook) or his employer's interests (e.g., as seen in *Shurgard*). This section begins with an overview of three approaches to the problem—authority as interpreted via agency, contract, and code—and suggests a consolidated approach through which to view these alternatives.

1. AUTHORIZATION GOVERNED BY AGENCY

Although *Shurgard* was its precursor, *International Airport Centers, L.L.C. v. Citrin*[98] is the marquee case for the agency-based interpretation of authorization. Jacob Citrin was an employee of a real estate-focused firm affiliated with International Airport Centers.[99] He was charged with identifying and assisting in the acquisition of properties presenting a favorable business opportunity to International Airport Centers.[100] Citrin was provided with a laptop to facilitate his work of identifying potential acquisition targets. When he

[96] *See* Black & Decker, Inc. v. Smith, 568 F. Supp. 2d 929, 936 n. 3 (W.D.Tenn. 2008); US Bioservices Corp. v. Lugo, 595 F. Supp. 2d 1189, 1193 n. 4 (D. Kan. 2009).

[97] *Black & Decker*, 568 F. Supp. 2d at 936 n. 3 (citing 18 U.S.C. § 1030).

[98] Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006).

[99] *Id.* at 419.

[100] *Citrin*, 440 F.3d at 419.

decided to quit, however, Citrin deleted all the data he collected and stored on the laptop, as well as data that would have revealed his improper conduct before deciding to quit. He also took additional steps to prevent the recovery of the deleted data.[101] International Airport Centers pursued a civil cause of action against Citrin under subsection 1030(a)(5)(A)(i), which prohibits intentionally causing damage without authorization to a protected computer.[102] In addition to this alleged violation, Judge Posner noted that Citrin's conduct also violated subsection 1030(a)(5)(A)(ii), which prohibits intentionally accessing a protected computer without authorization.[103] Relying upon the Restatement of Agency and *Shurgard*, the court found that by destroying the data that would have incriminated him, as well as other data belonging to his employer, Citrin acted in violation of the duty of loyalty that agency law imposes on employees.[104] Moreover, "Citrin's breach of his duty of loyalty terminated his agency relationship . . . and with it his authority to access the laptop, because the only basis of his authority had been that relationship."[105]

Both *Shurgard* and *Citrin* relied upon the RESTATEMENT (SECOND) OF AGENCY § 112.[106] This section deems the authority of an agent to terminate if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of duty.[107] The *Citrin* court also relied upon section 387 of the RESTATEMENT (SECOND) OF AGENCY.[108] This section notes that "[u]nless otherwise agreed, an agent is subject to a duty to his principal to act solely for the benefit of the principal in all matters connected with his agency."[109] Together, these principles establish a rule that would find

[101] *Id.* The data would have been easily recoverable if Citrin had not loaded the laptop with a secure-erase program.

[102] *Id.* This is now subsection 1030(a)(5)(A).

[103] *Id.* at 420. This is now subsection 1030(a)(5)(B).

[104] *Id.*

[105] *Id* at 420-21.

[106] *Id.* at 420; *Shurgard*, 119 F. Supp. 2d at 1124.

[107] RESTATEMENT (SECOND) OF AGENCY § 112 (1958).

[108] *Citrin*, 440 F.3d at 420.

[109] RESTATEMENT (SECOND) OF AGENCY § 387 (1958).

an employee to have acted without authorization when his intentions[110] became adverse to those of his employer.[111] This would be the case even if the employee had been given full technical access to use his employer's computer system. Thus, an employee acts with authorization when he acts in accordance with work-related functions, but loses such authorization when he acts against his employer's interests, such as to assist a competitor to his current employer's detriment. This interpretation of authority is unconcerned with the degree of technical access; rather, it looks to the nature of that access.

2. AUTHORIZATION GOVERNED BY CODE[112]

If an agency-based interpretation of authority can be said to favor the employer, a code-based interpretation surely favors the employee. In *Shurgard*, the defendant's principal argument was that the employee possessed technical access to view the data in question.

[110] Intent in this context should not be confused with the notion of acting intentionally, the mens rea needed to constitute most violations of the CFAA. *See, e.g.*, *supra* note 43 and accompanying text.

[111] In contrast, the RESTATEMENT (THIRD) OF AGENCY collapses these principles into a one-step mechanism for determining authority. Rather than authority becoming established via assent and then terminated pursuant to the acquisition of adverse interests or a serious breach of loyalty, a RESTATEMENT (THIRD) approach would hold that an agent "acts with actual authority when, at the time of taking action that has legal consequences for the principal, the agent reasonably believes, in accordance with the principal's manifestations to the agent, that the principal wishes the agent so to act." RESTATEMENT (THIRD) OF AGENCY § 2.01 (2006). Thus, the "focal point for determining whether an agent acted with actual authority is the time of action, not the time of the principal's manifestation, which may be earlier." *Id.* § 3.06, comment b. As one commentator has noted, this approach tightens some of the conceptual gaps in a *Citrin* analysis because it evaluates whether authority actually existed to begin with, as opposed to whether the circumstances were such to terminate it. Field, *supra* note 91, at 845 n. 155. However, as a practical matter, it would seem that the same circumstances that would terminate authority under RESTATEMENT (SECOND) would deem it not to have come into existence at all under RESTATEMENT (THIRD). Accordingly, the one-step approach does not seem to provide any meaningful advantage to the two-step approach aside from shifting the doctrinal vantage point.

[112] This interpretation of authority has heretofore been described as the "technological" or "narrow" interpretation. All three terms (i.e., code-based, technological, and narrow) are meant to reference the same model of interpretation, and are used interchangeably. Moreover, this interpretation pegs the legal definition of authorization to the physical degree of access that a user possesses. For example, a computer user who is *unable* to access a password-protected database because she does not know the password lacks *authorization* to access that database.

Based on this, the defendant reasoned, his access could not be deemed unauthorized. Although the *Shurgard* court rejected this interpretation, it has support among federal courts[113] and scholarly commentators.[114] The Ninth Circuit recently became the first federal appellate court to adopt this interpretation.[115] This narrower interpretation of authority holds that a violation for accessing data without authorization under the CFAA occurs only where initial access is not permitted.

In *LVRC Holdings v. Brekka*, LVRC, a residential addiction treatment center, hired Christopher Brekka to oversee multiple aspects of its facility, including internet marketing and coordinating with the website provider.[116] Brekka, however, also owned and operated two of his own consulting businesses at the time.[117] These businesses obtained referrals for addiction rehabilitation services and provided referrals of potential patients to rehabilitation facilities through websites and advertisements.[118] Because Brekka had to commute from Florida to Nevada, he often e-mailed work-related documents from his LVRC work computer to his personal computer in Florida.[119] This was not impermissible, as LVRC and Brekka did not have a written employment agreement and there existed no employee guidelines prohibiting him from doing so.[120] A month into his

[113] *See* Lewis-Burke Associates LLC v. Widder, No. 09-302 (JMF), 2010 WL 2926161, at *5 (D.D.C. July 28, 2010) (noting that the code-based line of cases has "recently gained critical mass"); Lockheed Martin v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *5 (M.D. Fla. Aug 1, 2006); Diamond Power Int'l v. Davidson, 540 F. Supp. 2d 1322, 1342 (N.D. Ga. 2007); Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 967 (D. Ariz. 2008); Brett Senior & Assocs., P.C. v. Fitzgerald, No. 06-1412, 2007 WL 2043377, at *4 (E.D. Pa. July 13, 2007); Int'l Ass'n of Machinists and Aerospace Workers v. Werner-Masuda, 390 F.Supp.2d 479, 498 (D. Md. 2005).

[114] *See* Kerr, *supra* note 17; Field, *supra* note 91; Brenton, *supra* note 51; Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164 (2004);, Greg Pollaro, *Disloyal Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope*, 2010 DUKE L. & TECH. REV. 12 (2010).

[115] *See* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1129-33 (9th Cir. 2009).

[116] *Id.* at 1129.

[117] *Id.*

[118] *Id.*

[119] *Id.*

[120] *Brekka*, 581 F.3d at 1129.

employment with LVRC, Brekka received an administrative username and password to LVRC's website.[121] With this login, he gained access to information about LVRC's website, including website usage statistics key to managing the firm's Internet marketing.[122] Two months later, Brekka and LVRC engaged in discussions regarding the possibility of Brekka purchasing an equity interest in LVRC.[123] He e-mailed himself LVRC data, including marketing budget information and a master admissions report, which included the names of past and current patients.[124] However, discussions soon broke down and Brekka left LVRC.[125] Two months later, while performing routine monitoring of the LVRC website, an administrator noticed that someone was accessing the usage statistics under Brekka's username.[126] LVRC deactivated his access and brought suit against Brekka, alleging a violation of subsections 1030(a)(2) and 1030(a)(4) arising from when he emailed LVRC documents to himself and continued to access the LVRC website after his employment ceased.[127]

In examining whether Brekka's access was unauthorized, the court looked first to the language of CFAA, noting that unless otherwise defined, words within statutes are to be interpreted as taking their ordinary, contemporary, common meaning.[128] Under this standard, the court found "permission or power granted by an authority" to be an appropriate denotation of authorization, and further found Brekka's access to meet this metric because LVRC gave him permission to use its computer.[129] The court reasoned, "when an employer authorizes an employee to use a company computer subject to certain limitations, the employee remains authorized to use the

[121] *Id.*

[122] *Id.*

[123] *Id.*

[124] *Id.* at 1129-30.

[125] *Brekka*, 581 F.3d at 1130.

[126] *Id.*

[127] *Id.* at 1129-30.

[128] *Id.* at 1132-33 (citing Perrin v. United States, 444 U.S. 37, 44 (1979)).

[129] *Id.* at 1133 (citing the Random House Unabridged Dictionary).

computer even if the employee violates those limitations."[130] Thus, access is unauthorized only when the employer decides to terminate it or when the employee did not have permission to begin with. Access exceeds authorization when a user has permission to access the computer but accesses information she is not entitled to access.[131] Because Brekka had permission to use the computer and did not lack permission to e-mail data to himself, he acted with authorization.[132]

In rejecting the *Citrin* approach, the *Brekka* court invoked the rule of lenity, noting that it is well established that ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity.[133] This method of narrow statutory construction requires courts to "limit the reach of criminal statutes to the clear import of their text and construe any ambiguity against the government."[134] Of course, the *Brekka* court was not the first or last to apply this principle of jurisprudence to the issue of authorization in the CFAA context.[135] In reaching outcomes consistent with *Brekka*, courts often have relied upon the lenity principle to find for the employee. Others, however, have rejected a defense rooted in the logic of lenity.[136]

[130] *Brekka*, 581 F.3d at 1133.

[131] *Id.*

[132] *Id.* The court then determined whether Brekka violated the CFAA by logging into the LVRC website after he left the firm. This inquiry indicates that the court did not employ a full code-based approach, but rather tempered it with its "permission" test. Under a complete code-based approach, this inquiry would have been superfluous–even though he left the firm, he still had an active login, meaning his access was still authorized.

[133] *Id.* at 1134-35; United States v. Bass, 404 U.S. 336, 347 (1971) ("Ambiguity concerning the ambit of criminal statutes shall be resolved in favor of lenity."). The rule of lenity is rooted in McBoyle v. United States, 283 U.S. 25, 27 (1931).

[134] *Brekka*. 581 F.3d at 1135.

[135] *See, e.g.*, Lewis-Burke Assocs. v. Widder, No. 09-302 (JMF) 2010 WL 2926161, at *5 (D.D.C. July 28, 2010); Orbit One Comm'ns, Inc. v. Numerex Corp., 692 F.Supp.2d 373, 386 (S.D.N.Y. 2010); Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 966-67 (D. Ariz. 2008); Lockheed Martin v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *7 (M.D. Fla. Aug. 1, 2006); Cenveo, Inc. v. Rao, 659 F. Supp. 2d 312, 316-17 n. 3 (D. Conn. 2009); US Bioservices Corp. v. Lugo, 595 F. Supp. 2d 1189, 1194 n. 5 (D. Kansas 2009); Brett Senior & Associates, P.C. v. Fitzgerald, No. 06-1412, 2007 WL 2043377, at *4 (E.D. Pa. July 13, 2007); Black & Decker, Inc. v. Smith, 568 F. Supp. 2d 929, 935 (W.D. Tenn. 2008).

[136] *See* United States v. Nosal, No. CR 08-00237 MHP, 2009 WL 981336, at 7 (N.D. Cal. Apr. 13, 2009); United States. v. John, 597 F.3d 263, 273 (5th Cir. 2010). The *Nosal* court noted that the rule of lenity is only appropriate when there is statutory ambiguity. *Nosal*,

In addition to the lenity principle, courts rejecting the *Citrin* approach have commonly invoked three additional arguments. First, courts have reasoned that because a CFAA violation is based upon a defendant's unauthorized *access* rather than her unauthorized *use*, a claim does not exist when an employee possesses technical access but harbors nefarious intent.[137] Second, courts have noted that the *Citrin* approach conflates the meaning of "without authorization" and "exceeds authorized access" in contravention of parameters established in section 1030(e)(6), which provides the statutory definition of the latter phrase.[138] The *Citrin* approach thus renders the distinction meaningless because both prongs are assigned the same meaning. Finally, courts have rejected the *Citrin* approach on account of legislative history.[139] Courts have noted that the statute's original aim was to create a cause of action against hackers, and that in support of its passage, the House Committee specifically noted that "Section 1030 deals with an 'unauthorized access' concept of computer fraud rather than the mere use of a computer."[140] In addition, courts have emphasized the fact that in 1986, Congress amended the statute to substitute the phrase "exceeds authorized access" in place of "having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does

2009 WL 981336, at *7. Applied to the CFAA, the court found the principle unavailing because there is no ambiguity in the statute. *Id.* Rather, "ample authority exists to permit criminal actions to proceed based on violations of [section 1030(a)(4)] by employees, as interpreted by civil cases, and there is simply no statutory basis to suggest otherwise." *Id.* (citing Shurgard Storage Ctrs. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1126 (W.D. Wash. 2000)). In light of *Brekka*, however, many of the government's CFAA claims were dismissed on the defendant's motion for reconsideration. United States v. Nosal, No. C 08-0237, 2010 WL 934257, at *9 (N.D. Cal. Jan. 6, 2010).

[137] *See, e.g.*, Int'l Ass'n of Machinists and Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 499 (D. Md. 2005); *Speed*, 2006 WL 2683058, at *5; Diamond Power Intern. v. Davidson, 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007) (citing *Speed*); *Black & Decker*, 568 F. Supp. 2d at 934 (citing *Speed*); *Lugo*, 595 F.Supp.2d at 1193.

[138] *See, e.g., Diamond Power Intern.*, 540 F.Supp.2d at 1342-43; *Gast*, 535 F. Supp. 2d at 965 (citing *Diamond Power Intern.*); *Lugo*, 595 F.Supp.2d at 1193; B & B Microscopes v. Armogida, 532 F.Supp.2d 744, 758 (W.D. Pa. 2007); *Speed*, 2006 WL 2683058, at *6.

[139] *See, e.g., Werner-Masuda*, 390 F. Supp. 2d at 495-96; *Gast*, 535 F. Supp. 2d at 965-66; *Black & Decker*, 568 F. Supp. 2d at 935-36.

[140] *See Gast*, 535 F. Supp. 2d at 965-66 (citing H.R. REP. NO. 98-894, at 20 (1984), *as reprinted in* 1984 U.S.C.C.A.N. 3689, 3706).

not extend."[141] By enacting this amendment, and by providing a definition for "exceeds authorized access," these courts have reasoned that congressional intent was contrary to the *Citrin* approach.[142]

3. AUTHORIZATION GOVERNED BY CONTRACT

The final type of interpretation focuses upon the breach of an express or implicit agreement to determine whether one's access is authorized or unauthorized. This interpretation is often invoked in cases concerning website terms of service agreements and employment agreements,[143] and stipulates that such contractual terms can define what constitutes authorized access. As one court recently noted, "[w]ithin the breach of contract approach, most courts that have considered the issue have held that a conscious violation of a website's terms of service/use will render the access unauthorized and/or cause it to exceed authorization."[144]

The contract-based interpretation is perhaps best understood through two First Circuit cases arising under the same facts.[145] Explorica, a company formed in 2000 to compete in the field of global tours for high school students, hired several former employees of EF, a company which had been engaged in the teenage tour market for more than thirty-five years.[146] Philip Gormley, Explorica's Chief Information Officer, previously Vice President of Information Strategy at EF, sought to gain a substantial advantage over firms like EF by

[141] *See id.* at 966; *Werner-Masuda*, 390 F. Supp. 2d at 499 n. 12 (quoting S. REP. NO. 99-432, at 9 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2486).

[142] *See Werner-Masuda*, 390 F. Supp. 2d at 499 n. 12 (quoting S. REP. NO. 99-432, at 21, 1986 U.S.C.C.A.N. at 2494-95); *Gast*, 535 F. Supp. 2d at 966.

[143] *See* Field, *supra* note 91, at 827-28.

[144] United States v. Drew, 259 F.R.D.449, 460-61 (C.D. Cal. 2009) (citing, among other cases, Register.com, Inc. v. Verio, *Inc.*, 126 F. Supp. 2d 238, 245-251 (S.D.N.Y. 2000), *aff'd* 356 F.3d 393 (2d Cir. 2004) and Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 450 (E.D. Va. 1998), and finding that an intentional breach of MySpace.com's terms of use agreement can potentially constitute accessing the MySpace computer/server without authorization and/or in excess of authorization under the CFAA).

[145] The two cases are EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001) and EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58 (1st Cir. 2003).

[146] *Explorica*, 274 F.3d at 580.

undercutting their prices on student tours.[147] This was achieved via a "scraper," a computer program used to access information contained in a succession of webpages stored on an accessed computer via the HTML source code which is available to anyone who views the website.[148] Explorica used its scraper to copy the price of each EF tour through every possible city.[149] After "scraping" two years of data from EF's website, Explorica set its own prices for tours, undercutting EF's prices by an average of five percent.[150] Upon learning of this practice, EF brought suit against Explorica, several Explorica employees, and Zefer Corporation, the company that designed and utilized the scraper, alleging violations of subsections 1030(a)(4), 1030(a)(5)(c), and 1030(a)(6)(A).[151]

Using a "reasonable expectations" test, the district court held that lack of authorization could be inferred from the circumstances and was so inferred on the basis of three such circumstances: (1) the copyright notice on EF's homepage with a link directing users to contact the company with questions; (2) the scraper's bypassing of technical restrictions embedded in the website permitting ordinary users to view the site only one page at a time; and (3) the likely violation of a confidentiality agreement between Gormley and EF arising because Gormley provided to Zefer technical instructions regarding the creation of the scraper.[152]

Although the *Explorica* court could have affirmed on the code-based violation, it chose instead to affirm on account of the broad confidentiality agreement Explorica's current, and EF's former, employees had violated.[153] The court held that EF's allegations, if true, would "likely prove that whatever authorization Explorica had to navigate around EF's website (even in a competitive vein), it exceeded

[147] *Id.*; *Zefer*, 318 F.3d at 61.

[148] *Zefer*, 318 F.3d at 60. A scraper is also known as a "robot" or "bot." *Id.*

[149] *Id.*

[150] *Id.*

[151] *Id.*

[152] *Id.* at 62; *Explorica*, 274 F.3d at 580-81.

[153] *Explorica*, 274 F.3d at 581-82. By affirming on these grounds, the court did not reach the question of whether the use of a scraper alone rendered the access unauthorized. *Id.*

that authorization by providing proprietary information and know-how to Zefer to create the scraper."[154]

In *Zefer*, the court added several important highlights to its opinion in *Explorica*. Here, no confidentiality agreement existed between Zefer and EF. In considering the application of a code-based approach, the court assessed the propriety of the district court's reasonable expectations test.[155] The court agreed that lack of authorization may be implicit, rather than explicit, but rejected reasonable expectations as a default rule in this context because it was "neither prescribed by the statute nor prudentially sound."[156] The court further noted that code-based interpretations of authorization may be deemed inconsistent with a test based upon reasonable expectations, pondering rhetorically "[w]hy should . . . the provision of page-by-page access . . . be taken to suggest that downloading information at higher speed is forbidden."[157] Although EF seemingly disliked the use of the scraper to construct Explorica's database, it would have equally disliked the compilation of such a database manually without the use of a scraper.[158] Moreover, the court preferred to require a public website provider to spell out explicitly what is forbidden, rather than put users at the mercy of a "highly imprecise, litigation-spawning standard like 'reasonable expectations.'"[159] An independent preliminary injunction against Zefer was unwarranted.[160]

[154] *Id.* at 583.

[155] *Zefer*, 318 F.3d at 62-64.

[156] *Id.* at 63. Notably, the court added: "password protection itself normally limits authorization by implication (and technology), even without express terms." *Id.*

[157] *Id.*

[158] *Id.* at 63. A prohibition against the latter would raise "serious public policy concerns." *Id.*

[159] *Id.* at 63. "If EF wants to ban scrapers, let it say so[.] [W]ith rare exceptions, public website providers ought to say just what non-password protected access they purport to forbid." *Id.* at 63-64. *But cf.* note 156, *supra* (leaving room for password protection to establish lack of authorization by implication).

[160] *Zefer*, 318 F.3d at 63. However, the injunction was affirmed because Zefer, as a defendant in the *Explorica* case, was on notice of the injunction and thus precluded from acting in concert with, on behalf of, or at the direction of Explorica to use the scraper to access EF's information. *Id.*

Courts examining whether authorization may be governed by contract have generally answered the question in the affirmative.[161] As a result, practitioners generally support the execution of employment agreements or explicit company policies defining, among other things, what access would be deemed authorized and what would be considered unauthorized.[162]

4. A CONSOLIDATED APPROACH

Although courts and scholars have addressed the three aforementioned interpretations as distinct, this article employs a dichotomous approach because the contract and agency-based approaches are identical in regard to their focus on what the employee intends to do via his access.[163] Thus, there are actually two approaches, not three. The distinction between them is based upon whether the employee's intent (e.g., to act on behalf of a competitor) or the employer's actions (e.g., erecting password protection) should be used as a basis for determining whether certain employee conduct is authorized or not.

The agency and contract-based interpretations focus upon the intentions of the employee. The key question is whether the employee is acting in accordance with the interests of her current employer, or instead harbors nefarious intent, such as the advancement of her own interests or those of another (future) employer. The contract-based interpretation fits within this category because, as one court aptly noted, the "common thread" in cases employing this interpretation is a focus on the employee's motive for accessing a computer and her

[161] *But see, e.g,.* Black & Decker, Inc. v. Smith, 568 F. Supp. 2d 929, 931-36 (W.D. Tenn. 2008) (finding that while employee had previously signed a confidentiality, termination, and employee access agreements with his former employer, he did not act lack authorization to copy a large volume of confidential and proprietary information from his former employer's secure servers via an external storage device and his personal email account because he had permission to access the information in question and doing so was within the scope of his duties).

[162] *See, e.g.*, Akerman, *supra* note 4; Bill Barnhart, Circuits Split Over Application of Computer Fraud Law, Dec. 1, 2009, InsideCounsel, *available at* http://www.insidecounsel.com/Issues/2009/December-2009/Pages/Circuits-Split-Over-Application-of-.aspx.

[163] Although "intent" is used throughout this article to describe the crux of this approach, it is also helpful to conceptualize this approach as focusing upon the employee's *purpose*–viz., whether or not the employee has acted in accordance with the duties and responsibilities associated with this work-related functions.

intended use of the information obtained.[164] Thus, within the employee's intent approach, agency-based and contract-based interpretations merely constitute a spectrum of legal doctrines to define authorization from the same focal point—the employee's intentions.

The alternative approach focuses on the employer and examines whether the employer, by his actions, has technically granted the employee permission to access a particular document or database. This approach primarily encompasses what has heretofore been referred to as the "code-based," "technological," or "narrow" interpretation of authorization. The key question under this approach is whether the employee was physically given access to employer information, often via a password or terminal. If an employee has not manipulated technological barriers to gain access to information (e.g., by using a stolen password or a coworker's computer), she is not in violation of the access element of the CFAA—even if her intention is to obtain her current employer's information solely for the benefit of a future employer who wishes to compete with her current employer.

This consolidated approach simplifies the issue of what constitutes "authorization." Part IV provides an overview of scholarly commentary relating to the interpretation of authorization.

IV. Literature Review

A review of the relevant scholarly commentary provides an important backdrop to interpreting authorization because it expands the issue from a discrete question to one which necessary implicates larger theoretical debates, such as criminal law in the digital context and the debate regarding the merit of a cyberproperty regime.[165] These areas of inquiry overlap with commentary assessing the merits of the three aforementioned interpretations of authorization and provide helpful guidance in resolving the immediate question of what constitutes authorization.

The two scholars whose views on the interpretation of authorization seem to have gained the most traction among courts both endorse the adoption of a code-based approach but differ in the

[164] Brett Senior & Assocs., P.C. v. Fitzgerald, No. 06-1412, 2007 WL 2043377, at *4 (E.D. Pa. July 13, 2007); *see also* Richard Raysman & Peter Brown, *'Unauthorized Access' Under Computer Fraud, Abuse Act*, N.Y. L.J., Apr. 8, 2008, at 3 (noting the same in regard to the *Citrin* line of cases).

[165] *See supra* note 25.

mechanical aspects of such an approach and its supporting rationale.[166] Professor Kerr argues that courts should reject contract-based notions of authorization, and instead limit the scope of unauthorized access to the circumvention of code-based restrictions.[167] Professor Kerr's proposed framework would require courts to interpret "access" broadly: "A user accesses a computer any time the user sends a command to that computer that the computer executes."[168] This approach would define "access" as any successful interaction with a computer.[169] Kerr draws support for this interpretation of access on account of the following: Because technology will continue advancing, this approach will eliminate access as a limit on the scope of unauthorized access statutes, and place considerable weight on the meaning of authorization.[170] This broad approach to access would be balanced by limiting the phrase "without authorization" to the circumvention of code-based restrictions.[171] Kerr advances instrumental,[172] historical,[173] and

[166] *See* Kerr, *supra* note 17, at 17; Bellia, *supra* note 114. Kerr and Bellia are not the only commentators to endorse a code-based approach. *See, e.g.*, Brenton, *supra* note 51, at 460; Field, *supra* note 91, at 819; *see also* Mary W. S. Wong, *Cyber-trespass and 'Unauthorized Access' as Legal Mechanisms of Access Control: Lessons from the US Experience*, 15 INT'L J. L. & INFO. TECH. 90, 125 (2007) (considering alternative approaches unwise); Nicholas R. Johnson, *"I Agree" to Criminal Liability: Lori Drew's Prosecution Under §1030(A)(2)(C) of the Computer Fraud and Abuse Act, and Why Every Internet User Should Care,* 2009 J.L. TECH. & POL'Y 561, 583-88 (2009) (discussing *Drew* and suggesting a code-based approach). Kerr and Bellia, however, seem to lead when considering judicial reliance on their work (i.e., citations).

[167] Kerr, *supra* note 17, at 1644; *see also* Lemley, *supra* note 25, at 528 ("An even more serious problem is the judicial application of the [CFAA], which was designed to punish malicious hackers, to make it illegal—indeed, criminal—to seek information from a publicly available website if doing so would violate the terms of a [contractual] license."). Kerr would also reject an agency-based approach. Kerr, *supra* note 17, at 1632 (referring to *Shurgard* as "strikingly broad").

[168] Kerr, *supra* note 17, at 1646.

[169] *Id.* at 1646-47.

[170] *Id.* at 1647-48.

[171] *Id.* at 1644. Access would be deemed "without authorization" only when it violates the *Morris* intended function test, or else uses false identification to trick the computer into granting the user greater privileges. *Id.* at 1649. For a discussion of this test, see note 91 *supra*.

[172] *Id.* at 1644. It would allow Internet users to enjoy as much freedom as possible to do as they wish online and protect the privacy and security of Internet users and their data. *Id.* In

doctrinal[174] rationales in support of this interpretation of authorization. Finally, Kerr cautions that a contract-based approach would "allow . . . a computer owner to harness the criminal law at his discretion, using his unilateral power to control authorization by contract as a tool to criminalize any viewpoint or status the owner wishes to target."[175]

Professor Bellia reaches the same conclusion, arguing that "only breach of a code-based control on access should trigger liability" under the CFAA.[176] Bellia's proposed interpretation differs from Kerr's first in terms of how "access" should be defined. While Kerr endorses a broad reading of the term, Bellia finds a narrow reading to be more "natural."[177] This reading focuses "not merely on the successful exchange of electronic signals, but rather on conduct by which one is in a position to obtain privileges or information not available to the general public."[178] Bellia further drifts from Kerr by providing textual arguments to support her thesis. She points to several prohibitions in the CFAA that contemplate obtaining generally unavailable information, such as national security information and financial and

contrast, a contract-based approach would "grant computer network owners too much power to regulate what Internet users do, and how they do it, sacrificing a great deal of freedom for a small gain in privacy and security." *Id.* at 1650.

[173] Kerr, *supra* note 17 at 1649.

[174] *Id.* at 1652. It tracks the traditional treatment that analogous issues have received in criminal law, namely in the interpretation of consent defenses for crimes such as burglary, trespass, and rape. *Id.* at 1652-54.

[175] *Id.* at 1658-59 (using an example of a pro-life network owner whose Terms of Use agreement allows only those who express pro-life opinions to use the network, thus exposing pro-choice users to criminal liability).

[176] Bellia, *supra* note 114, at 2234. This is an application of her larger thesis that "property-rule protection for network resources is more appropriate than scholars have thus far recognized." *Id.* at 2170 (noting that the weight of scholarship supports liability rule). Moreover, Bellia argues that "entitling a system owner to property-rule protection so long as she provides the user with actual notice of permissible uses of the system or adopts a system configuration making it plain to the user that access is restricted would better balance the interests of consumers and system owners than rejecting property-rule protection outright." *Id.* at 2164.

[177] *Id.* at 2254. Professor Kerr relies was relying upon a conception of "authorization" to supply a limiting principle, whereas Bellia would also finds an outer boundary in "access." *See supra* notes 167-70 and accompanying text.

[178] *Id.* at 2253-54.

other records.[179] If access without authorization "is to be read consistently throughout the statute," Bellia argues, "then it must extend only to breaches of these sorts of code-based limitations."[180] Bellia draws additional support for a narrow reading from legislative history, arguing that nothing indicates Congressional intent to extend the statute's application to publicly available information.[181]

Other commentators have expressed reservations as to the adoption of a code-based interpretation. One scholar has noted that such an interpretation of unauthorized access is "flatly inconsistent with the explicit language of [the CFAA], which makes a clear distinction between 'unauthorized access' and 'access in excess of authorization'," and "flatly inconsistent" with the post-1986 legislative history of the statute.[182] Furthermore, policy rationale may also caution against code-based interpretations. As Professor Winn argues, the code-based interpretation artificially restricts the set of norms that courts are permitted to consider to those prevalent among computer programmers.[183] According to Winn, the fact that a code-based model would yield inequitable results compounds this concern. Specifically, "a homeowner who simply fails to secure a personal computer [via code protections] should still be entitled to the protection of computer

[179] *Id.* at 2254. Since the information is not publicly available, it is necessarily segregated by code or placed on a system not generally accessible to the public. *Id. But see* Galbraith, *supra* note 31, at 335 ("Despite the fact that the CFAA's legislative history suggests that the statute is designed to protect confidential information, as opposed to all other types of information, the statutory language is not so limited.").

[180] Bellia, *supra* note 114, at 2254.

[181] *Id.* at 2257. Rather, she notes, the legislative record continually stressed issues of security and confidentiality. *Id.* Others, however, have found the statute's legislative history ambiguous. *Cf.* Field, *supra* note 91, at 830 (reviewing legislative history and finding that "because the legislative history contains independent support for [contract-, agency-, and code-based interpretations], no single approach is justified on the grounds that it represents the congressionally dictated interpretation of authorization."). Field goes on to note, however, that taking a broader approach to the CFAA's legislative history reveals a legislative aim to create liability for computer misuse, and a code-based approach best approximates that aim. *Id.* at 835-37. Field adds that because Congress exhibited evasiveness and ambiguity when dealing with the issue of insider authorization, it may have intended to leave the question of authorization in employment situations for courts to decide. *Id.* at 840-41.

[182] Winn, *supra* note 3, at 1419.

[183] *Id.* Winn calls this a system of "norms by nerds."

trespass laws against an unwanted intrusion into his or her home computer system."[184]

Beyond endorsing a particular interpretation of a key term, some commentators have advanced legislative approaches to the problem by advocating the repeal or revision of the CFAA's private cause of action as a means to limit expansive interpretation of the statute.[185]

Finally, some commentators have compared the CFAA to alternative means of protection. While some have argued that the CFAA's goal of protecting information "has been, and continues to be, fulfilled quite adequately by existing 'traditional' criminal statutes,"[186] others have cited the broad and expansive nature of the CFAA as justification to minimize the need for other additional protections against electronic trespass.[187]

Distinctly lacking from the CFAA debate is a prolonged discussion regarding the application of the statute in the employment context.[188] Commentators generally seem opposed to such an application, particularly when employee intent governs the interpretation of authorization.[189] The next part addresses the question: Which is a

[184] *Id.* at 1420.

[185] Brenton, *supra* note 51, at 457 (suggesting that Congress either amend the CFAA to remove the subsection (a)(2)(C) from the ambit of the private right of action or add a statutory definition of the term "authorization" that overturns the *Shurgard/Citrin* reading of the statute); Galbraith, *supra* note 31, at 366-68 (arguing that because the CFAA was meant to deter hackers, not to control access to, and use of, information on publicly available websites, the statute should be amended to ensure such access and use without statutory liability).

[186] Olivenbaum, *supra* note 23, at 624 (arguing that "[traditional criminal statutes] are likely to be more effective vehicles for the prosecution of computer-related crimes," and adding that "[s]tatutes that focus instead on the technical means by which a prohibited result may be achieved tend to be unnecessary, imprecise, and quickly outstripped by changing technology.").

[187] Michael A. Carrier & Greg Lastowka, *Against Cyberproperty*, 22 BERKELEY TECH. L.J. 1485, 1513-15 (2007) (arguing that the scope, statutory detail, and history of the CFAA minimizes the need for cyberproperty to protect against electronic invasion).

[188] The only scholarly commentary directly focused on this has been Field, *supra* note 91; and Winn, *supra* note 3.

[189] *See* Field, *supra* note 91, at 821, 825; Kerr, *supra* note 17, at 1596; Dan E. Lawrence, Comment, *Just Add Plaintiff: The Seventh Circuit's Recipe for Instant Liability Under the Computer Fraud and Abuse Act*, 46 WASHBURN L.J. 223, 243 (2006) (arguing that *Citrin* has potential to extend liability to actors outside Congress's intended scope because it resulted from the court's misunderstanding of the relevant technology involved). *But see* Richard Warner, *The Employer's New Weapon: Employee Liability Under the Computer*

more prudent basis for interpreting authorization, employer conduct or employee intent?

V. CRITICAL APPRAISAL OF THE COUNTERVAILING INTERPRETATIONS OF "AUTHORIZATION"

A. THE EMPLOYER'S CONDUCT OR THE EMPLOYEE'S INTENT

An employer's conduct approach certainly has appeal in that the use of code and similar hard-line, technical barriers provides an easy rule for courts to apply. Either an employee can physically access data, or she cannot. Thus, code forms a binary proxy for authorization and the basis of liability with few, if any, exceptions. This regime, however, also has disadvantages.

The immediate appeal of an employee's intent approach is that it captures all of the wrongful accessers.[190] The appeal of this approach is well-framed in the inverse: Simply stated, "[w]hy should an employee who oversteps the bounds of his or her permission to transfer sensitive information to a third party, or the third party that receives such information, not be liable?"[191] It is no easy feat to vindicate an IRS employee who uses the IRS system in violation of strict confidentiality restrictions to obtain the tax returns of his political enemies, their family members, a former girlfriend, and a prosecutor charging his father with an unrelated felony.[192] Similarly, should an account manager at a trusted firm escape liability under the CFAA when she provides co-conspirators with her client's confidential account information in order to transact fraudulent purchases?[193] Without some consideration of the employee's intent, these rogue employees would escape the reach of the CFAA.

Fraud and Abuse Act, 12 EMP. RTS. & EMP. POL'Y J. 11, 27-28 (2008) (supporting an agency-based approach).

[190] Lockheed Martin Corp. v. Speed, 81 U.S.P.Q.2d 1669, 1675 (M.D. Fla. 2006).

[191] *See* Warner, *supra* note 189, at 28.

[192] United States v. Czubinski, 106 F.3d 1069 (1st Cir. 1997). Although the employee "unquestionably exceeded authorized access," his misuse did not satisfy the statutory requirement that he obtain "anything of value." *Id.* at 1078.

[193] United States v. John, 597 F.3d 263 (5th Cir. 2010) (holding that she should not).

B. Implementation Costs and Gains

An employer's conduct approach carries with it high infrastructure costs that will probably be passed on to end-users. Code technology must be acquired, installed, updated, and maintained. Total *economic* costs probably exceed actual financial costs. This is because code or similar technical barriers necessarily slow the pace of operations, as employees must regularly enter passwords to access the data needed for work-related functions, thus incurring opportunity costs. Although a central administrator could be charged with this function, this simply shifts this burden rather than eliminating it. Therefore, a legal regime based upon an employer's conduct entails costs beyond that of the technology itself, and such costs may neither be explicit nor easily quantifiable. Despite these concerns, a legal rule that leads to increased expenses should not be eschewed solely on that basis. It is perhaps more prudent to ask who would play the role of the cheapest cost avoider.[194] Under such a framework, the burden should fall upon the employee, who knows—and controls—when he will cause harm, as opposed to the employer, who, unaware of how or when an employee may cause harm, must protect against all possible vulnerabilities.[195]

The asymmetry of information present in the employment relationship[196] is exacerbated in this particular context because the costs to the employer of bad bargaining are far greater than those conventionally associated with contracting for employment (i.e., malicious intent potentially imposing high economic costs as opposed to poor work quality and/or ethic). Monitoring, which is costly on its

[194] This concept was expounded in Guido Calabresi, The Costs of Accidents: A Legal and Economic Analysis (1970).

[195] *But see* Brenton, *supra* note 51, at 461 (arguing that because the employer is in the best position to determine who should have access to his company's systems, he should bear the burden of determining who has authorized access for the purpose of the statute). Brenton's argument fails to consider the fact that the ability to determine who should have access for work-related functions is different from the ability to determine who may abuse that access, how they may do so, and when.

[196] *See* Walter Kamiat, *Labor and Lemons: Efficient Norms in the Internal Labor Market and the Possible Failures of Individual Contracting*, 144 U. PA. L. REV. 1953, 1957-59 (1996) ("An employee and employer contracting for employment fits [a market for lemons] model: each possesses unique access to information—information regarding the quality of their offers—that the other party would find highly relevant, but which neither party can easily discover from the other."); Edward B. Rock & Michael L. Wachter, *The Enforceability of Norms and the Employment Relationship*, 144 U. PA. L. REV. 1913, 1924 (1996).

face,[197] seems less effective in the context of a rogue employee than with a shoddy worker.[198] In the seemingly analogous context of intentional torts, Judge Posner has shown further cause to quell doubt that the employee is the cheapest cost avoider in this context: The rogue employee, like the intentional tortfeasor, should be deemed the cheapest cost avoider because his cost of avoiding damage or loss to his employer is negative.[199] Rather, he must expend resources in order to carry out his malicious plans. In this sense, his cost of avoidance is less than that of his employer, who instead must incur positive costs to thwart the efforts of any and all potentially rogue employees.[200]

Additionally, as a practical matter, the employer's conduct approach simply does not solve the problem of rogue employees. As one court noted:

> While passwords and other electronic means can limit the unauthorized dissemination of some confidential information, an employee who has not yet announced his departure is still able to access confidential information and store it on a CD or floppy disk before he or she leaves . . . [and/or] quickly transmit information out of the company via e-mail.[201]

Even if an employer has put in place a robust system of code-based access and has demarcated each employee's access to that data necessary for him to fulfill his work-related responsibilities, the

[197] *See* Rock & Wachter, *supra* note 196, at 1924 ("Firms can learn by monitoring, but constant monitoring is very costly. To save on costs, firms infrequently monitor workers.").

[198] Presumably, a worker cannot hide shoddy work product longer than he can disguise malicious intent, as one is more readily detectable than the other.

[199] William M. Landes & Richard A. Posner, THE ECONOMIC STRUCTURE OF TORT LAW 149-60 (1987). This description is adopted from Alon Harel, *Efficiency and Fairness in Criminal Law: The Case for a Criminal Law Principle of Comparative Fault*, 82 CAL L. REV. 1181, 1197-1199 (1994).

[200] Landes & Posner, *supra* note 199, at 149-60.

[201] Pacific Aerospace & Electronics, Inc. v. Taylor, 295 F. Supp. 2d 1188, 1196 (E.D. Wash. 2003). This loophole would presumably diminish the deterrent power of computer crime law in the employment context. *See* Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169, 207-08 (1968) (arguing that a rational criminal would violate the law when his expected gain from violating a criminal statute would exceed the expected penalty).

employer still cannot protect against an employee misappropriating accessible data. In *Continental Group, Inc. v. KW Property Management, L.L.C.*, for instance, the court observed that although an employer's computer system had tiered levels of access governed by employees' use of usernames and passwords, the defendant employee's access level was high enough to be able to access all the files she was accused of misappropriating.[202]

A code-based or similar approach draws lines in the wrong places and puts the burden on employers to predict the necessary questions of who, when, what, and how. The result is a legal framework as superfluous as the technical framework to which it attaches. The resulting legal regime doctrinally assumes that one who is given a key can do no harm to that which he is granted access. Such an assumption is clearly out of touch with the issues encountered in the aforementioned cases, and with current issues in the employment relationship.[203] Without some focus on the employee's intent, the employer's conduct approach seems to place an impossible burden on employers, and inappropriately tilts the balance in the employee's favor.

The employer's intent approach avoids the incurrence of inefficient infrastructure expenses lacking attendant gains. Compared to the employer, the rogue employee is the cheaper cost avoider. This is because the expenditure of technological security measures creates numerous costs, including the technology itself, as well as the slowdown in the pace of workflow that would result from technological barriers. An interpretation of authorization focusing on employee's intent would be cheaper because the legal framework would itself provide adequate protection without the need for an additional trigger mechanism (e.g., an unpermitted code bypass). There is no reason to suspect that agency costs, such as monitoring, bonding, and residual costs, would exceed those already present in the employment relationship.[204]

[202] 622 F. Supp. 2d 1357, 1372-73 (S.D. Fla. 2009).

[203] *See supra* Part II, Subpart A.

[204] "Monitoring costs" are costs that employers (principals) expend to ensure employee (agent) loyalty. "Bonding costs" are costs that employees expend to ensure employers of their reliability. "Residual costs" are costs arising from differences of interest that remain after monitoring and bonding costs are incurred. *See* Michael C. Jensen & William H. Meckling, *Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure*, 3 J. FIN. ECON. 305, 308 (1976).

C. CONGRESSIONAL INTENT

The statutory structure and legislative history favor an employee's intent approach. An employer's conduct approach is inconsistent with the statutory structure of the CFAA, specifically with the statute's dichotomy of access violations. It is difficult to envision how any technical framework an employer can implement may differentiate between violations arising from lack of any authorization (i.e., "without authorization") and violations arising from insufficient authorization (i.e., "exceeding authorized access"). Either an employee has breached a code barrier, or she has not. Because any bypass of a technical barrier would need to be deemed access without authorization, the two degrees of violation would be rendered superfluous. It is a well-settled canon of statutory construction to avoid such a result.[205] The most plausible explanation for this dichotomy under an employer's conduct approach would be that all employee-related violations of the CFAA fall within the latter category because employees are initially granted at least some access. However, such an approach removes the *Citrin* fact pattern from the employer's remedies because subsection 1030(a)(5) does not include a provision for exceeding authorized access. Thus, an employee would not face liability under the CFAA if, prior to quitting and joining a competitor, she intentionally deleted sensitive data on her employer's computer system. It is difficult to accept such an approach because subsection 1030(a)(5) violations seem to be the most culpable. Deleting sensitive data, and thus depriving the employer of it, is worse than copying that data because value is impermissibly destroyed as opposed to impermissibly transferred. In the former instance, it would be absurd to argue that the employee lacked reason to believe that what he was doing was forbidden.

Although the employee's intent approach also faces conceptual challenges in light of the statutory distinction between access without authorization and access in excess of authorization, the notion of exceeding access may be viewed as a means of prohibiting improper use. For instance, an employee may have access to view her client's credit card information but may exceed that access when she does so in furtherance of an identity theft scheme. This control on intended use is unnecessary in regard to the subsection 1030(a)(5) violations because there is no *intended* way to destroy an employer's sensitive

[205] *See* Beck v. Prupis, 529 U.S. 494, 506 (2000) (recognizing that "terms in a statute should not be construed so as to render any provision of that statute meaningless or superfluous.").

resources. Some courts have opposed this reasoning, noting that an employee's intent approach conflates unauthorized access with unauthorized use, which is not prohibited on the face of the statute.[206] However, these courts have neglected to observe that an interpretation of authorization focused on the employer's conduct, which they endorse, conflates authority with ability, a conceptual leap. Furthermore, under an employer's conduct approach it is difficult to separate authority and access because, under such an approach, if an employee is given access, she has authority. Thus, an employee violates the CFAA if she accesses without access. This conflation is particularly egregious considering the fact that any construction of the statute depends on these terms conveying distinct meanings. Nevertheless, the employee's intent approach is undermined by the fact that the 1986 amendments revised the statutory text to remove from the statute's ambit circumstances in which an employee's access is legitimate in some instances but criminal in other (not clearly distinguishable) instances.[207] This, however, is the only piece of legislative history distancing congressional intent from an employee's intent approach.[208] Subsequent amendments and general themes of the legislative history favor an employee's intent approach.

An employer's conduct approach is also inconsistent with the CFAA's legislative history. As others have concluded, the legislative history provides few hints as to which interpretation of authorization was intended.[209] Reviewing the legislative history contextually, however, Katherine Mesenbring Field notes that "[b]ecause code serves as the primary constraint on behavior . . . circumventing code protections must be categorized as the misuse of a computer," which is what the CFAA was originally conceived to address.[210] However,

[206] *See supra* note 137 and accompanying text.

[207] *See supra* note 45 and accompanying text.

[208] It is curious that other important pieces of legislation have uniquely adapted themselves to the nascent field of employment law. For instance, although the Employee Retirement Income Security Act of 1974, 29 U.S.C. §§ 1001-1461, was aimed at private employer pension plans with little explicit attention to health plans, over time the statute was used to preempt an increasing number of state regulations affecting employment-based health plans, without any effort by Congress to overrule such interpretations. *See* MARK A. ROTHSTEIN & LANCE LIEBMAN, EMPLOYMENT LAW 495-501 (6th ed. 2007).

[209] *See* Field, *supra* note 91, at 829-34; *supra* note 181 and accompanying text.

[210] *See* Field, *supra* note 91, at 834-38. Computer misuse stands in opposition to traditional crimes using computers. *Id.*; Kerr, *supra* note 17, at 1602-05.

although originally designed to punish and deter hackers, the CFAA has been robustly expanded since its original enactment in 1984.[211] These expansions were accompanied with congressional prerogative to paint with a broad stroke. Senator Patrick Leahy, chair of the subcommittee on Technology and the Law of the Committee on the Judiciary, for instance, acknowledged this when he remarked:

> On the day we pass a law, we are, in effect, taking a snapshot of what we know that day. But however we draw it, somebody is going to sit down and say, well, look, I am just going to create a variation not covered by the statute. I am not sure all of us, putting our best minds together, could come up with every variation on a law that might get enacted some time this year to cover some new variation next year.[212]

Senator Leahy's remarks clearly suggest that the CFAA should be construed broadly to accommodate new varieties of computer-related crime and compensate for Congress's inability to predict them.[213] This

[211] Lawrence, *supra* note 189, at 239 ("There seems to be a congressional mandate that courts interpret the CFAA broadly."); *see supra* notes 56-57 and accompanying text.

[212] Lawrence, *supra* note 189, at 239 n.144 (citing The Impact of Computer Viruses and Other Forms of Computer Sabotage or Exploitation on Computer Information Systems and Networks: Hearing Before the Subcomm. on Technology and the Law of the Comm. on the Judiciary, 101st Cong. 12 (1989) (statement of Sen. Patrick Leahy)). Furthermore, this reasoning is neither unique nor exclusive to the cybercrime context. See SEC v. Edwards, 540 U.S. 389, 393 (2004) ("[The definition of an investment contract] 'embodies a flexible rather than a static principle, one that is capable of adaptation to meet the countless and variable schemes devised by those who seek the use of the money of others on the promise of profits.'") (quoting SEC v. Howey, 328 U.S. 293, 299 (1946)). Indeed, in regulating the securities market, Congress "painted with a broad brush" and defined the term "security" in "sufficiently broad and general terms[.]" Reves v. Ernst & Young, 494 U.S. 56, 60-61 (1990).

[213] *Id.*; *see also* U.S. v. Mitra, 405 F.3d 492, 495 (2005) ("[A]lthough legislators may not know about [a particular computer-based radio networking system], they *do* know that complexity is endemic in the modern world and that each passing year sees new developments. That's why they write general statutes rather than enacting a list of particular forbidden acts. And it is the statutes they enacted—not the thoughts they did or didn't have—that courts must apply.") (emphasis in original); *Decker*, *supra* note 35, at 1011, 1015-16 ("As computers continue to evolve in their methods of creation and storage of valuable information, Congress must again modernize the criminal provisions to protect this irreplaceable commodity[.] The Internet is constantly shape shifting, and it is impossible to foresee the nature and scope of all of the opportunities now and in the future for cyber criminals.").

should entail a focus not upon what an employer has done to prevent unauthorized access, but on what the employee seeks to achieve by his actions. Thus, a code-based approach imprudently confines the CFAA's protection within formalistic barriers and puts the burden on employers to continually erect these barriers to renew their statutory protection.

The legislative history of the CFAA supports the claim that Congress designed the statute broadly with the intention that it be sufficiently malleable to address new, emerging threats that arise through the improper use of a computer. Such flexibility is consistent with the approach Congress took in enacting a single statute to address the problem of computer misuse. Thus, as with the mail and wire fraud statutes upon which the CFAA was modeled,[214] it is prudent and legally sound to use the CFAA as a first line of defense to address new forms of serious crime that do not fall within more specific legislation.[215] Although the threat of computer hackers was a significant concern in 1984 (when the statute was enacted), today there is reason to suspect that the threat posed by hackers has been overstated.[216] On the contrary, employee sabotage and disloyalty is a new, serious crime that leaves employers vulnerable to those who have the greatest access, knowledge of operations, and ability to do harm. Not only do alternative remedies not provide sufficient protection,[217]

[214] *See supra* note 92 and accompanying text.

[215] United States v. Czubinski, 106 F.3d 1069, 1079 (1st Cir. 1997) (citing United States v. Maze, 414 U.S. 395, 405-06 (1974) (Burger, C.J., dissenting) ("When a 'new' fraud develops—as constantly happens—the mail fraud statute becomes a stopgap device to deal on a temporary basis with the new phenomenon, until particularized legislation can be developed and passed to deal directly with the evil.")).

[216] Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 U.C. DAVIS L. REV. 1327, 1331 (2008) (arguing that there is unwarranted focus on hackers and looking to the unauthorized computer access controversy as one area where rhetoric has driven policy despite lack of empirical evidence); Reid Skibell, *The Myth of the Computer Hacker*, 5 INFO. COMM. & SOC'Y 336, 347-53 (2002) (explaining that the hacker threat is inflated, arising from, among other things, the film *WarGames*, and noting that "insiders are a far greater threat than external attacks.").

[217] *See* Diamond Power Int'l v. Davidson, 540 F. Supp. 2d 1322,1334-35 (N.D. Ga. 2007) (employer not afforded trade secret protection—or CFAA claim—against former employee who misappropriated for the benefit of a rival employer an extensive list of approximately 35,000 parts and raw materials used to produce his current employer's products, despite the existence of a confidentiality agreement, password protection, and physical security measures); Mercer Mgmt. Consulting, Inc. v. Wilde, 920 F. Supp. 219, 235 (D.D.C. 1996) (employer denied breach of fiduciary duty claim when former senior employees mailed diskettes containing prior work to two major clients in order to increase clients' comfort

Congress specifically intended legal overlap.[218] Adopting an interpretation of authorization that is tied to existing technology would do precisely that which Congress has cautioned against—anchoring the CFAA to current technology when technology is consistently developing.[219]

D. Doctrinal Foundations

A regime based on employer conduct lacks a proper doctrinal basis for liability. Professor Kerr supports his proposal for a code-based interpretation by arguing that criminalizing circumvention of code tracks the traditional treatment of consent defenses in criminal law.[220] He notes, "the computer is 'tricked' into authorizing the defendant to access the computer, in a way conceptually similar to how a homeowner might be tricked into allowing a person into their home or a victim might be tricked into consenting to a request to engage in sexual activity."[221] He further draws a distinction between fraud in the inducement, which does not legally invalidate consent and resembles contract-based restrictions, and fraud in the factum, which invalidates consent and resembles a code-based restriction.[222] This makes sense if the CFAA is viewed as a statute seeking to criminalize traditional crimes using a computer. However, the CFAA is better viewed as a statutory response to crimes of computer misuse.[223] This legislative aim ventures into the terrain of cyberproperty and the notion that "code is law," a concept popularized by Professor Lessig which posits

level in switching their business from employer to a competing firm the former employees joined).

[218] S. Rep. No. 104-357, at 7-8 (1996) ("[W]here the information stolen is also copyrighted, the theft may implicate certain rights under the copyright laws.").

[219] *See* Olivenbaum, *supra* note 23, at 624 ("Statutes that focus . . . on the technical means by which a prohibited result may be achieved tend to be unnecessary, imprecise, and quickly outstripped by changing technology."); *see also supra* notes 212-13 and accompanying text.

[220] Kerr, *supra* note 17, at 1652 (citing examples of trespass, burglary, rape, and sexual assault).

[221] *Id.* at 1654.

[222] *Id.* at 1652-56.

[223] *Id.* at 1602; Field, *supra* note 91, at 836. For an overview of the distinction, see *supra* note 24.

that computer code may be understood as either equivalent to, or interchangeable with, the power of law.[224] The normative appeal of this proposition, however, is at least questionable. If accepted, the competing sovereignty of code recognized under this theory would threaten to undermine the rule of law.[225] According to Professor Lastowka, when faced with new technologies such as network exclusion, the law can provide several different responses. It might offer legal alternatives to the power of exclusion, legally prohibit technological exclusion, or ignore the new technology altogether.[226] He provides the following example:

> Cars, for instance, are not laws. Car ownership gives the owner the technological ability to drive quickly and endanger the lives of others. However, the law intrudes, to curb the right to exercise technological power (via speed limits), to regulate who can exercise that power (by licensing), and to provide special civil penalties for failing to follow social directives regarding the use of the power (e.g. driving while intoxicated).[227]

An interpretation of authorization that permits an employer's use of code to supplant law provides a questionable doctrinal foundation upon which to govern the employment relationship. At the very least, some mix of legal and technological exclusion rules is more appropriate.[228]

An employee's intent approach to interpreting authorization avoids the messy intermingling between technology and law. Rather, an employee's intent approach—particularly the *Citrin/Shurgard* interpretation—unites the CFAA with agency law doctrine, which

[224] Greg Lastowka, *Decoding Cyberproperty*, 40 IND. L. REV. 23, 24 (2007). Professor Lessig elaborated on his theory in LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

[225] *See* Lastowka, *supra* note 224, at 58 n.216 (citing Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 543 (1999) ("Code writers can write code that displaces the values that law has embraced. And if the values of law are to survive, law might well have to respond.")).

[226] *Id.* at 60.

[227] *Id.*

[228] *Id.*

governs the employer-employee relationship, and also contract law, which similarly plays a key role in the relationship. All employees are agents of their employer (the principal), in accord with the definition of employee in section 7.07 of the RESTATEMENT (THIRD) OF AGENCY (2006).[229] Thus, this interpretation provides a well-settled doctrinal foundation to the concept of authorization.

E. THE RULE OF LENITY

Although some commentators have argued that an employee's intent approach serves to criminalize the law of contract when the use of a computer is involved,[230] under proper circumstances a breach of contract can constitute a crime.[231] Moreover, agency law principles are not divorced from the criminal context.[232] In fact, some crimes require a breach of fiduciary duty in order to trigger criminal liability.[233] Thus, some courts have reasoned imprudently that the rule of lenity forecloses consideration of employee's intent as the proxy for authorization within the meaning of the CFAA. The Supreme Court

[229] RESTATEMENT (THIRD) OF EMPLOYMENT § 1.01 cmt. a (Tentative Draft No. 1, 2008).

[230] *See* Brett Senior & Assoc. v. Fitzgerald, 26 I.E.R. Cases 674, 677-78 (E.D. Pa. 2007) (employee's breach of a confidentiality agreement); Kerr, *supra* note 17, at 1600.

[231] For instance, an employee who steals trade secrets, breaching a confidentiality agreement, can also be guilty of violating the Economic Espionage Act of 1996. *See* Akerman, *supra* note 4; Lorin L. Reisner, *Transforming Trade Secret Theft Violations into Federal Crimes: The Economic Espionage Act*, 15 TOURO L. REV. 139, 139 (1998).

[232] *See Carpenter v. United States*, 484 U.S. 19, 27-28 (1987) (citing RESTATEMENT OF AGENCY to support conviction of journalist who divulged prepublication confidential information of employer in violation of the mail and wire fraud statutes); United States v. Galindo, 871 F.2d 99, 101 (9th Cir. 1989) (holding that although defendant was entitled to receive mail on account of employee status, her taking mail with intent to steal ended agency relationship and she was guilty of theft even though she converted mail to her own use thereafter); United States v. Hill, 579 F.2d 480, 482 (8th Cir. 1978) (reasoning that if defendant intended to convert a check when he removed principal's mail, his agency terminated).

[233] Insider trading law has been construed in accordance with agency law principles. *See* A.C. Pritchard, United States v. O'Hagan: *Agency Law and Justice Powell's Legacy for the Law of Insider Trading*, 78 B.U. L. REV. 13 (1998) (arguing that United States v. O'Hagan, 521 U.S. 642 (1997) establishes a foundation for insider trading based on agency principles). Pritchard favors agency law over the classical theory of insider trading, which draws heavily on the law of deceit because "[a]gency law provides a more comprehensive and coherent basis for dealing with the problem of insider trading, which is, at bottom, the misuse by faithless agents of information that belongs to others." *Id.* at 17.

has increasingly watered down its formulation of the lenity rule, applying it only in the face of "grievous ambiguity," or only if "after seizing everything from which aid can be derived," the Court can make "no more than a guess as to what Congress intended."[234] In reality, "[t]he simple existence of some statutory ambiguity, however, is not sufficient to warrant application of that rule, for most statutes are ambiguous to some degree."[235] Rather, lenity should be reserved for situations in which "a reasonable doubt persists about a statute's intended scope even *after* resort to 'the language and structure, legislative history, and motivating policies' of the statute."[236] Considering Congress's apparent desire to affect a broad sweep with the CFAA, the rule of lenity seems to offer a less instructive tool. Moreover, disregarding the Supreme Court's recent jurisprudence, it is difficult to bring the common rogue employee fact pattern within the ambit of the rule of lenity because the employee who breaches an explicit agreement or who violates clear terms of service was given fair warning that the conduct she engaged in was forbidden.[237] A counterargument should focus only on the extent of repercussions, not whether punishment is warranted.

F. VAGUENESS AND OVERBREADTH

Professor Kerr's scholarship has drawn attention to two constitutional problems that may emerge from the application of an employee's intent theory of authorization.[238] First, a contract-based

[234] Note, *The New Rule of Lenity*, 119 HARV. L. REV. 2420, 2423-24 (2006) (collecting cases).

[235] Muscarello v. United States, 524 U.S. 125, 139 (1998) (holding that the phrase "carries a firearm" as used in a criminal statute is not limited to the carrying of firearms on one's person, but also applies to possessing of firearms in one's vehicle).

[236] Moskal v. United States, 498 U.S. 103, 108 (1990) (emphasis in original).

[237] In United States v. John, 597 F.3d 263, 272-73 (5th Cir. 2010) for instance, the Fifth Circuit rejected a lenity argument, reasoning that interpreting the CFAA in accordance with an employee's intent approach would not be "unexpected" because "[a]n authorized computer user 'has reason to know' that he or she is not authorized to access data or information in furtherance of a criminally fraudulent scheme." Although *John* presents an extreme case (misappropriating customer account information in order to incur fraudulent charges), it is difficult to argue that an explicit employment agreement, for instance, provides any less "reason to know" something is impermissible than does a criminal statute.

[238] Kerr, *supra* note 17; Kerr, *supra* note 3.

interpretation of authorization may permit a network owner to "harness the criminal law at his discretion," thus creating overbreadth concerns arising from the unilateral power to control authorization.[239] As Professor Winn argues, however, there is reason to believe that such fears are premised on a misunderstanding of trespass doctrine, which has never given owners the arbitrary power to determine what access to their property is authorized.[240] Rather, "[w]here the use of an ostensibly private resource serves a socially beneficial purpose with little harm to the interests of the property owner, the common law recognizes exceptions to the general principle of the requirement of permission."[241] Thus, conceptualizing the CFAA as a statute concerning digital trespass (an understanding that runs in accord with congressional intent),[242] and applying well-settled doctrinal principles to its scope,[243] should eliminate, or at least dramatically temper, problems relating to overbreadth.

Second, Kerr argues that an agency-based interpretation of authorization is susceptible to void-for-vagueness arguments.[244] In other CFAA contexts, however, this argument has failed to persuade most of the courts that have considered it.[245] In *United States v. Mitra*, for instance, the defendant contended that the CFAA was not

[239] Kerr, *supra* note 17, at 1658. Kerr provides the example of a student conducting research on the Ku Klux Klan who accesses a KKK website by clicking "I Agree" to a terms of use agreement conditioning authorization to access the site on adherence to racist beliefs. *Id.* at 1622-23.

[240] Winn, *supra* note 3, at 1422.

[241] *Id.* at 1422-23 (noting further that "the severity of the common law of trespass is constantly lessened by privileges, licenses and immunities as a matter of law to protect reasonable public use of the ostensibly private resource"); *see, e.g.,* New Jersey v. Shack, 277 A.2d 369 (N.J. 1971).

[242] *See supra* notes 25-26 and accompanying text.

[243] *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1072 (2003) (citing Beck v. Prupis, 529 U.S. 494, 500-01 (2000) for the proposition that federal statutes are to be interpreted in light of the common law, and looking to the common law of trespass to guide its interpretation of the Stored Communications Act).

[244] Kerr, *supra* note 3, at 1583-87.

[245] Most courts confronted with the vagueness argument have rejected it. *See* United States v. Mitra, 405 F.3d 492, 496 (7th Cir. 2005); United States v. Powers, 2010 WL 1418172, at *4 (D. Neb. Mar. 4, 2010); United States v. Kernell, 2010 WL 1543847, at *3-*7 (E. D. Tenn. Apr. 7, 2010), *aff'd in part, rev'd in part,* 2010 WL 1544281 (E. D. Tenn. Apr. 19, 2010). *But see* United States v. Drew, 259 F.R.D. 449, 467 (C.D. Cal. 2009).

meant to target his interference with a computer-based radio system.[246] Judge Easterbrook rejected his vagueness argument, reasoning that the defendant's problem is "not that [the CFAA] has been turned in a direction that would have surprised reasonable people; it is that a broad statute has been applied *exactly as written*, while he wishes that it had not been."[247] Although no court seems to have directly encountered a vagueness challenge to an agency-based interpretation of authorization applied in the context of a rogue employee case, there is no reason to suspect such challenges will fare better than previous vagueness challenges to the CFAA. Congress had employees in its sights when it enacted the CFAA,[248] and it sought a broad evolution of the statute to address new challenges that may arise in the future.[249] Accordingly, a broad interpretation of authorization is consistent with the statute's purpose and purview, and should not be deemed unconstitutional on vagueness grounds.[250]

[246] *Mitra*, 405 F.3d at 496. When summarizing the crux of his argument, the court noted that, in contrast to an ex-employee erasing data on his employer's system, Congress could not have intended for Mitra's conduct to constitute a violation of the CFAA. *Id.* at 495 (citing United States v. Lloyd, 269 F.3d 228 (3d Cir. 2001)).

[247] *Id.* ("There is no constitutional obstacle to enforcing broad but clear statutes[.] The statute itself gives all the notice that the Constitution requires.") (emphasis in original); *see also* United States v. Councilman, 418 F.3d 67, 85 (1st Cir. 2005) (rejecting vagueness challenges and noting that "[a]lthough the text of the statute does not specify whether the term 'electronic communication' includes communications in electronic storage, the legislative history of the [Electronic Communications Privacy Act of 1986] indicates that Congress intended the term to be defined broadly.").

[248] *See supra* notes 92-97 and accompanying text.

[249] *See supra* notes 56-57, 212-13, 219 and accompanying text; *see also Mitra*, 405 F.3d at 495 ("Section 1030 is general. [Statutory] [e]xclusions show just *how* general[.] As more devices come to have built-in intelligence, the effective scope of the statute grows. This might prompt Congress to amend the statute but does not authorize the judiciary to give the existing version less coverage than its language portends.") (emphasis in original); Winn, *supra* note 3, at 1435 ("When courts have interpreted the broad statutory language in the CFAA in ways Congress has determined to be inconsistent with public policy, it has quickly taken steps to limit those decisions with specific language.").

[250] *See* Akerman, *supra* note 4 (noting that although the wire fraud statute could be used to prosecute a student who calls home interstate asking his parents for school money when he instead intends to use it to buy alcohol, this potential for misuse of prosecutorial discretion has not prompted anyone to seriously argue that the statute is unconstitutional).

G. DOWNSIDE PROTECTION

Potential problems arising from an employee's intent interpretation are less severe than those caused by an employer's conduct approach.

At least one commentator has expressed concern that an agency-based approach creates potential for judicial manipulability and "disparate outcomes" because agency principles leave room for judicial discretion.[251] This argument proves too much. The common law itself may be characterized as a legal regime that specifically contemplates a role for judge-made rules. Within this regime, a flexible legal rule should be preferred in an area characterized by rapid development of technology, such as the law of computer network integrity. As Professor Richard A. Epstein has noted, "new forms of technology create the opportunity for new forms of resource use. . . . A common law system that is able to work itself pure should be able to respond to these changes both by preserving what makes sense in the older system and by changing what does not."[252] Implicit fairness considerations[253] and the safeguard of appellate review further ease reservations as to the prudence of judicial discretion in this area.

Adopting an employee's intent approach also would not be a venture into uncharted legal terrain. Jurisdictions outside the U.S. have found merit in an interpretation of authorization focusing on employee's intent. Courts in the United Kingdom, Australia, and

[251] Field, *supra* note 91, at 844-45.

[252] Richard A. Epstein, *Cybertrespass*, 70 U. CHI. L. REV. 73, 73-74 (2003).

[253] *Cf.* Wong, *supra* note 166, at 127 (discussing cyberproperty cases and noting that "it is possible to view the courts' actions, simply, as doing the right thing once the plaintiff presents a convincing case that her interests are in need of a legal remedy."). In *Shurgard* and *EF Cultural,* although the employers had the power to restrict the employees' access, they lacked reason to suspect that such actions were necessary. The employees were still employed by their respective firms when the violations occurred. For *Shurgard, see supra* notes 67-78 and accompanying text. For *EF Cultural, see supra* notes 146-51 and accompanying text. The *Brekka* opinion, by contrast, suggested that the employment relationship differed from that of a conventional one and LVRC was in a better position to safeguard its interests than similarly situated employers. *See supra* notes 116-27 and accompanying text. This argument suggests that CFAA cases may be best understood through a standards- rather than rules-based framework. Thus, the governing legal metric is an ex post, rather than ex ante, assessment of the actor's conduct. For a useful overview of the distinction between rules and standards, see Kathleen M. Sullivan, *Foreword: The Justices of Rules and Standards*, 106 HARV. L. REV. 22, 57-59 (1992).

Singapore, for instance, have looked to a user's intent to determine whether her access lacks authorization.[254]

VI. CONCLUSION

Employers should be afforded broad safeguards under the CFAA. An interpretation of authorization that focuses upon employee's intent is the better approach to achieve these ends. The implementation of this goal is probably best achieved through legislative amendment to the CFAA.[255] In particular, section 1030(e) should be amended to add a definition to the term "authorization." This definition should be structured in such a way so as to conform to the employee's intent interpretation. Additionally, because Congress's attempts to define the difference between insider and outsider violations have proven unworkable, the distinction between access "without authorization" and access "exceeding authorization" should be omitted from the statute. The statute should only prohibit access without authorization. Thus, congressional intent to apply the CFAA to insiders, such as employees, would be preserved, though it would no longer be spelled out on the face of the statute. Jurisdictions outside the United States have enacted statutes identical to the CFAA without expressly including offenses that depend upon a person having exceeded their authority. These jurisdictions have prosecuted insiders using general statutory proscriptions against accessing without authorization.[256] Because this alteration of the CFAA is an amendment of the statute's actual language and structure, it cannot be achieved through judicial rule. Legislative amendment will better alleviate any concerns regarding the rule of lenity and vagueness because any ambiguity will be definitely resolved and fair warning will be provided to potentially rogue employees.

[254] *See* Winn, *supra* note 3, at 1409-10 (discussing the United Kingdom and Australia); Wong, *supra* note 162, at 119-22 (discussing the United Kingdom and Singapore).

[255] Alternatively, the Supreme Court could weigh in on the issue and thus resolve the circuit split. However, statutory amendment seems the more prudent approach.

[256] *See* Wong, *supra* note 166, at 121-22.